AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

wanda522@hotmail.com, as further described in Attachment A-1, and Sony Y Series laptop, as further described in Attachment A-2

Case No. MJ18-071

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Hotmail Account and Sony Series Laptop as further described in Attachment A-1 and A-2, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1 and B-2, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 371, 1001, 1028A, 1546, and 1341	Conspiracy to Defraud the United States, False Statements, Aggravated Identity Theft, Visa Fraud, and Mail Fraud

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT MICHAEL RUFFIER, U.S. STATE DEPT
Printed name and title

Sworn to before me and signed in my presence.

Date: 2-21-18

Judge's signature

City and state: SEATTLE, WASHINGTON

PAULA L. MCCANDLIS, U.S. MAGISTRATE JUDGE
Printed name and title

2016R00055

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, MICHAEL RUFFIER, a Special Agent with the Diplomatic Security Service (DSS) in Seattle, Washington, having been duly sworn, state as follows:

AFFIANT BACKGROUND

1. I am a Special Agent of the Diplomatic Security Service ("DSS"), which is an agency of the United States Department of State ("State Department"), and I have been so employed for over 8 years. I am presently assigned to the Seattle Resident Office. I am empowered under 22 U.S.C. § 2709 to investigate visa frauds, as well as to apply for and serve federal arrest and search warrants. My previous assignments with DSS include the San Francisco Field Office, U.S. Embassy Baghdad, Iraq, U.S Consulate Ho Chi Minh City, Vietnam, and the Seattle Resident Office, along with numerous long-term temporary duty assignments to locales throughout the Middle East and South Central Asia. I also have a Bachelor's Degree in Business from the University of Oregon.

INTRODUCTION AND PURPOSE OF AFFIDAVIT

2. This Affidavit is submitted in support of an application for warrants to search the following places for evidence of violations of Title 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1546(s) (visa fraud), and 18 U.S.C. § 1341 (mail fraud) (collectively the "Specified Federal Offenses"). The SUBJECT LOCATIONS are described in additional detail in Attachments A-1 and A-2 to this Affidavit and Application, which are attached hereto and incorporated by this reference:

a. The email account wanda522@hotmail.com (the "SUBJECT EMAIL ACCOUNT"). The email account is owned and controlled by Barbara Tomaszewski, who prepared petitions for H-1B visas that Divensi and its sister company

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Azimetry, Inc. ("Azimetry") sent to the United States Citizenship and Immigration Services ("USCIS") between approximately 2012 and 2014. The information associated with the SUBJECT EMAIL ACCOUNT is stored at premises controlled by Microsoft, Inc., an email provider headquartered in Redmond, Washington. This affidavit seeks the authority under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Microsoft, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B. Upon receipt of the information described in Section I of Attachments B-1, government-authorized persons will review that information to locate the items described in Section II of Attachment B-1.[1]

b. A Sony Y Series laptop bearing model number PCG-31311L, which is presently stored at the offices of Aoki Law PLLC at 1200 Fifth Avenue, Suite 750, Seattle, Washington 98101 (the "**SUBJECT LAPTOP**"). The SUBJECT LAPTOP belongs to Prasad Puvvala ("Puvvala") the former Chief Operations Officer of Divensi, Inc. Puvvala has informed the Government that Divensi provided him with the laptop and gave him permission to keep it for his personal use upon his departure from the company. Puvvala also informed the Government that he is willing to consent to the search of his laptop. Nonetheless, in an abundance of caution against the possibility that Divensi did not, in fact, provide Puvvala with permission to keep the laptop and consent to its search, the Government seeks authority to forensically examine the SUBJECT LAPTOP for the purpose of identifying electronically stored data, which is particularly described in Attachment B-2.

3. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§2703(a),

[1] On or about January 30, 2018, the Government sent Microsoft, Inc. a preservation letter requesting that all emails and associated files for the SUBJECT EMAIL ACCOUNT be preserved for 90 days. On February 5, 2018, Hotmail responded confirming receipt and compliance with the requests set out in the preservation letter.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(b)(1)(a), and (c)(1)(a). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offenses being investigated." 18 U.S.C. § 2711(3)(a)(i).

4. The facts set forth in this Affidavit are known to me as a result of my participation in this investigation, from information provided to me by other law enforcement officers and from records, documents, and other evidence obtained during this investigation. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested search warrants, I have not included each and every fact known to me concerning this investigation, but rather those facts which I believe are necessary to establish probable cause to search the SUBJECT LOCATIONS. Everything set forth in this Affidavit is true to the best of my knowledge and belief.

STATEMENT OF PROBABLE CAUSE

5. Divensi and Azimetry provide information-technology services to corporate clients, including a variety of so-called "Fortune 500" companies (and recruiting firms retained by those companies), in the information-technology field. More specifically, at all times relevant to this investigation, Divensi and Azimetry have hired employees with experience in the information-technology field, such as programmers, marketed those employees to corporate clients, and then placed those employees at corporate clients pursuant to contracts entered into between Divensi and Azimetry and their clients (and/or their clients' agents). Many of the employees who Divensi and Azimetry hired and then placed at their corporate clients entered into the United States under specialty-occupation ("H-1B") visas, which Divensi and Azimetry petitioned for in applications filed with the United States Citizenship and Immigration Services (USCIS).

6. Since early 2015, the United States Department of State has investigated Divensi and Azimetry for numerous suspected false statements in petitions for H-1B visas, which those companies sent to USCIS. On September 29, 2017, the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington, issued search warrants authorizing law-enforcement agents to search the offices of Divensi and Azimetry under cause number MJ17-413. The Affidavit submitted

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

in support of the applications for those warrants is attached hereto as Exhibit A and incorporated in its entirety as if set forth herein.[2] As set out in Exhibit A, there is probable cause to believe that Divensi and Azimetry together submitted approximately one-hundred-and-forty (140) petitions for H-1B visas containing false statements. In particular, the petitions falsely claimed that the intended foreign-national beneficiaries of the requested visas already had been assigned to work on projects for two corporate clients named Revel, Inc. ("Revel") and GeoDigital, Inc. ("GeoDigital"). The applications attempted to support these false assertions by using fabricated letters, which were attached to the applications and which purported to have been signed by agents of Revel and GeoDigital. Rather than assign the visa beneficiaries to work on projects for Revel and GeoDigital, Divensi and Azimetry marketed (and eventually placed) those employees at other corporate clients.

7. In the two sub-sections below, I supplement Exhibit A with the facts that establish probable cause to believe that the SUBJECT LOCATIONS contain evidence of the crimes under investigation.

A. Facts Establishing Probable Cause to Search the SUBJECT EMAIL ACCOUNT

8. As set out in Exhibit A, Pradyumna Samal ("Samal") has always owned Divensi and Azimetry and has served as the Chief Executive Officer ("CEO") of both companies. Emails found in Samal's and Puvvala's email accounts, as well as the email accounts of other employees and executives and the companies, establish that the companies recruited foreign nationals (who either lived abroad or already lived in the United States pursuant to a valid visa), petitioned for H-1B visas for those employees by making false statements, and then marketed those foreign workers to actual end clients after they entered the United States. The companies collected the margin between the

[2] The Affidavit (Exhibit A) itself incorporated by reference an earlier affidavit submitted in support of an application to search certain business email accounts for Divensi and Azimetry, which resulted in the issuance of search warrants by the Honorable Brian A. Tsuchida, United States Magistrate Judge for the Western District of Washington, under cause numbers MJ16-194 and MJ16-313.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

price they charged end clients for foreign workers' services and the salary that they paid those foreign workers.

9. Emails found in Divensi's and Azimetry's accounts show that Tomaszewski helped the companies prepare the visa petitions and appeared to charge the companies a per-petition fee for her services.[3] As noted in Exhibit A, public records show that Tomaszewski was formerly a licensed attorney in Washington State, who was disbarred from the practice of law in 1998 and later expelled from the practice of law before the Department of Homeland Security in 2002.

10. Despite her earlier disbarment and expulsion, emails show that Tomaszeski helped prepare the vast majority of the visa petitions submitted by Divensi and Azimetry between 2012 and 2014. Indeed, when law-enforcement agents interviewed her on October 6, 2017, Tomaszewski admitted that she has worked for Samal and various companies that he owned since 2002 and on an *ad hoc* basis. More specifically, Tomaszewski admitted that she assembled and filed H-1B visa petitions for Divensi and Azimetry. Tomaszewski also admitted that the petitions included purported letters from Revel and GeoDigital, for the proposition that the foreign workers would work for those companies.

11. There is probable cause to believe that the SUBJECT EMAIL ACCOUNT contains evidence regarding the process by which the visa petitions filed by Divensi and Azimetry were prepared, including how the false documents within those petitions were drafted, edited, and compiled before mailing. Tomaszewski herself admitted on October 6, 2017 that she used the SUBJECT EMAIL ACCOUNT to communicate with her clients at Divensi and Azimetry regarding visa petitions. She also admitted that she used the SUBJECT EMAIL ACCOUNT to conduct immigration-related work for Divensi and Azimetry. In addition to Tomaszewski's own admissions, other evidence found in the course of the investigation shows that Tomaszewski used the SUBJECT EMAIL ACCOUNT to perform her work for Divensi and Azimetry:

---

[3] The Affidavit (at Exhibit A) refers to an "outside consultant" who helped prepare visa petitions. *See, e.g.*, Affidavit, ¶ 28 (referring to a March 19, 2014 email from an "outside consultant" regarding materials included in a visa petition relating to a foreign worker referred to as "A.K."). Tomaszewski is that "outside consultant."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Emails found in Divensi's and Azimetry's email accounts, as well as emails found on Tomaszewski's personal laptop (which was searched pursuant to her consent) show that Tomaszewski sent digital copies of petition documents to Samal, Puvvala, and others at the companies, along with instructions about how to compile those documents before mailing them to USCIS. For instance, on March 19, 2014, the SUBJECT EMAIL ACCOUNT emailed Samal and Puvvala regarding a petition for a foreign worker referred to as "A.K.," and attached a petition and purported end-client letter issued by Geodigital, stating (falsely) that "A.K." would work for Geodigital upon arrival in the United States. In the body of the email, Tomaszewski told Samal and Puvvaala to "find the forms, etc. for [A.K.]" and instructed them about how to mark the outside of the envelope to USCIS. In another email, on May 1, 2013, the SUBJET EMAIL ACCOUNT asked Divensi's accounting manager to confirm details regarding a foreign-worker who was the subject of a pending visa petition, which claimed (falsely) that the worker would be assigned to a project for Revel upon entry into the United States.

b. There is also probable cause to believe that the SUBJECT EMAIL ACCOUNT was specifically involved in transmitting (either in draft or final form) the false and forged end-client letters that Divensi and Azimetry included in their petitions. For instance, on March 16, 2013, the SUBJECT EMAIL ACCOUNT sent Samal and Puvvala an email that attached letters that purported (falsely) to have been issued by Revel, and which claimed (falsely) that to different foreign workers would be assigned to projects for Revel upon arrival in the United States. Tomaszewski also used the SUBJECT EMAIL ACCOUNT to send Samal unsigned versions of those false and forged end-client letters along with a request for "signed" versions of the attachments, which Samal then produced.

12. In an email sent in or about June 2017, the current immigration attorney for Divensi and Azimetry informed law enforcement that "Barbara" – an apparent reference to Tomaszewski – worked in house as an employee for Divensi and Azimetry when

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

preparing visa petitions for those companies. However, the available evidence suggests that Tomaszewski in fact worked as an outside contractor for Divensi and Azimetry, and that she used her own personal email address, rather than any company-issued email address, to perform services for the companies.

B. Facts Establishing Probable Cause to Search the SUBJECT LAPTOP

13. As set out in Exhibit A (and above), Divensi and Azimetry's employees and Tomaszewski used digital devices extensively in order to prepare, circulate, and then submit visa petitions that contained false and forged documents. Puvvala participated in the visa-preparation process, as evidenced by his inclusion and participation in email conversations in which he asked Samal to sign end-client letters, circulated draft documents for inclusion in visa petitions, and guided foreign-worker beneficiaries about how to navigate visa interviews.

14. On January 30, 2018 and February 5, 2018, Puvvala agreed to be interviewed in Seattle, Washington. Part of the interview was conducted pursuant to a proffer agreement entered into between the Government and Puvvala. During the interviews, Puvvala confirmed that he worked as the COO for Divensi between 2012 and 2015. Puvvala also confirmed that he helped prepare visa petitions that Divensi and Azimetry filed using his company-issued laptop, i.e., the SUBJECT LAPTOP.

15. Puvvala stated that he continued to possess the SUBJECT LAPTOP, which he had stored at his residence in India, where he now lives. At the Government's request, Puvvala asked a member of his household in India to mail the SUBJECT LAPTOP to his attorney, Russ Aoki, Esq., at Mr. Aoki's offices in Seattle, Washington. Puvvala said that Divensi and Azimetry permitted him to keep the SUBJECT LAPTOP for his personal use after he left the company, but that the SUBJECT LAPTOP continued to have files on it that related to his work at the company, including his work preparing visa petitions.

16. Puvvala told the Government that he was willing to consent to the search of the SUBJECT LAPTOP, but the Government nonetheless seeks a warrant to search the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUBJECT LAPTOP in an abundance of caution. At the Government's request, the SUBJECT LAPTOP is currently being stored at the offices of Russ Aoki, Esq., in Seattle, Washington. Mr. Aoki has told the Government that, upon the issuance of a warrant for the search of the computer, he will surrender the laptop to law-enforcement agents.

17. There is probable cause to believe that the SUBJECT LAPTOP contains evidence of the crimes under investigation for all of the reasons set out in Exhibit A, namely that Puvvala helped prepare and submit false visa petitions, he sent the documents in those petitions over email, and he communicated with others at (and outside) the company over email with regard to those petitions. Those facts make clear that Puvvala used digital devices, and the SUBJECT LAPTOP in particular, when participating in the process of preparing visa petitions.

BACKGROUND REGARDING EMAIL PROVIDERS' SERVICES

18. In my training and experience, I have learned that Microsoft, Inc. provides the public with a variety of on-line services, including electronic mail ("email") access, to the public, including through the Hotmail service. Subscribers obtain an account by registering with Hotmail. During the registration process, Microsoft asks subscribers to provide basic personal information, which may include name, address, phone numbers, payment information, and other personal information.

19. Microsoft's computers are likely to contain stored electronic communications (including retrieved and unretrieved email) and information concerning subscribers and their use of Hotmail's services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

20. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

21. In general, an email that is sent to a subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time.

22. When subscribers send emails, they are initiated at the users' computers, transferred via the Internet to the Microsoft's servers, and then transmitted to their end destinations. Microsoft often maintains a copy of the email sent. Unless the email senders specifically delete the emails from Microsoft's servers, the emails can remain on the systems indefinitely. Even if the senders delete the emails, they may continue to be available on Microsoft's servers for a certain period of time.

23. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Microsoft but may not include all of these categories of data.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

24. Subscribers to Microsoft's services can also store files, including emails, address books, contact or buddy lists, calendar data, photographs, and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, attachments to emails, including photographs and files, and photographs and files stored in relation to the account.

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. This application seeks a warrant to search all responsive records and information under the control of Microsoft, which is subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

27. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities on a digital device, namely the SUBJECT LAPTOP. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

29. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer forensics examiners, and my training and experience, I submit that there is probable cause to believe that the SUBJECT LAPTOP contains evidence of the crimes under investigation, and indeed has been used as an instrumentality of those offenses. For the reasons explained above, there is probable cause to believe that Puvvala used the SUBJECT LAPTOP to compile documents in visa petitions and to circulate those documents to others associated with Divensi and Azimetry.

30. There is, therefore, probable cause to believe that evidence of the crimes under investigation exist and will be found on the SUBJECT LAPTOP, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes under investigation, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT LAPTOP because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF THE SUBJECT LAPTOP

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

33. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

or otherwise copying the SUBJECT LAPTOP, and will specifically authorize a later review of the media or information consistent with the warrant.

34. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of the SUBJECT LAPTOP, and to conduct off-site searches of the SUBJECT LAPTOP thereafter:

Processing the Search Sites and Securing the Data.

a. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT LAPTOP.[1]

b. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the SUBJECT LAPTOP.

c. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to

---

[1] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

Searching the Forensic Images

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

REQUEST FOR SEALING

35. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, affidavit and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation and disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Disclosure of these materials would give the target of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

36. Based on the foregoing, there is probable cause that the Subject Companies have committed violations of 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1546(a) (visa fraud), and 18 U.S.C. § 1341 (mail fraud). I request the issuance of search warrants authorizing the search of the SUBJECT LOCATIONS for evidence, instrumentalities, and fruits of the Specified Federal Offenses and the seizure of those items whether in electronic or non-electronic form.

Michael Ruffier, Affiant
Special Agent
Diplomatic Security Service
U.S. Department of State

Subscribed to before me this 21 day of February, 2018.

PAULA L. MCCANDLIS
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Description of Property to be Searched

This warrant applies to information associated with the email addresses wanda522@hotmail.com, including all preserved data associated with the account and all subscriber and log records associated with the account, which is located at premises owned, maintained, controlled, or operated by Microsoft, Inc., a company headquartered in Redmond, Washington.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Description of Property to be Searched

A Sony Y Series laptop bearing model number PCG-31311L, which is presently stored at the offices of Aoki Law PLLC at 1200 Fifth Avenue, Suite 750, Seattle, Washington 98101.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

Items to Be Seized

I. Information to be disclosed by Microsoft, Inc. (the Provider):

To the extent that the information described in Attachment B-1 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. §2703(f), the Provider is required to disclose the following information to the government, within fourteen (14) days of the issuance of this warrant:

a. The contents of all emails and instant messages associated with the account(s), including stored or preserved copies of emails or instant messages sent to and from the account(s) (including header information), draft emails or instant messages, deleted emails or instant messages which are still available, the source and destination addresses associated with each email or instant message, the date and time at which each email or instant message was sent, and the size and length of each email or instant message;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the IP address used to register the account(s), log-in IP addresses associated with session times and dates, account status, alternative email addresses provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service(s) utilized;

d. All records or other information stored at any time by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. All records pertaining to communications between the Provider and any person regarding the account(s), including contacts with support services and records of actions taken;

f. All records available regarding the location of the user of the account(s), including information obtained from IP addresses, GPS, wifi access points, or cell towers;

g. All records regarding device-specific information for devices used to access the accounts, including hardware model, operating system version, unique device identifiers, and mobile network information, including phone numbers;

h. Records of any other accounts associated with the SUBJECT ACCOUNTS through common cookies, device identifiers, email addresses, or phone numbers; and

i. Web and search history information for the accounts.

For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

II. Information to be seized by the government:

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1546(s) (visa fraud), and 18 U.S.C. § 1341 (mail fraud) (collectively the "Specified Federal Offenses"), those violations occurring between 2012 and 2015, including information pertaining to the following matters:

1. All records, messages, documents, log files, and other information regarding the identity of the creator, user(s), or individual(s) controlling the SUBJECT EMAIL ACCOUNT, and their past, present, or future location;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. All records, messages, documents, log files, and other information regarding the identity of individuals being communicated with in regards to the above listed violations, and their past, present, or future location;
3. All messages, documents, and other information, including messages sent or received, all attachments, documents, or other information regarding:
    a. Files, records, and other items relating to applications for visas and other forms of legal status in the United States, including but not limited to, visa applications and attachments, drafts of visa applications and attachments, information regarding the preparation of visa applications and attachments, correspondence relating to visa applications and attachments, material (e.g., contracts, offer letters, job specifications) used in visa applications and attachments, notes and other contemporaneous documents regarding visa applications and attachments; and discarded material evidencing false documents and information in visa applications and attachments;
    b. Files, records, and other items relating to employees, including but not limited to offers of employment, employment contracts, Security Deposit Agreements, Master Services Agreements, Statements of Work, resumes, wage or salary information, employment offers, travel documents, identification documents, records relating to dates of retention and termination; and discarded material evidencing false documents and information with regard to employment or contracting relationships;
    c. Files, records, and other items relating to the marketing of employees, including but not limited to marketing materials, memoranda regarding employees, staffing calendars, worker schedules, timesheets, attendance records, interview schedules, requests for specialized labor from prospective clients;
    d. Files, records, and other items relating to financial transfers with foreign-national employees and/or clients or vendors with which those employees

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

were placed, including records showing the wiring or transfer of money or currency from copies of checks and/or actual wire transfer instructions, wire receipts, and/or bank account records showing the wiring or transfer of money via check or wire.

4. Evidence indicating how and when the SUBJECT EMAIL ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

5. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

6. Any address lists or buddy/contact lists associated with the specified account;

7. All subscriber records associated with the specified account, and any other accounts accessed from the same computers or digital devices, including:

   a. name,

   b. address,

   c. records of session times and durations,

   d. length of service (including start date) and types of service utilized,

   e. subscriber number or identity, including any temporarily assigned network address, and

   f. means and source of payment for such service) including any credit card or bank account number; and

Any and all other historical log records, including IP address captures, associated with the specified account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-2

Items to Be Seized

Evidence, fruits, and/or instrumentalities of the commission of the following crimes: 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1546(s) (visa fraud), and 18 U.S.C. § 1341 (mail fraud) (collectively the "Specified Federal Offenses"), those violations occurring between 2012 and 2015, including:

a. Files, records, and other items relating to applications for visas and other forms of legal status in the United States, including but not limited to, visa applications and attachments, drafts of visa applications and attachments, information regarding the preparation of visa applications and attachments, correspondence relating to visa applications and attachments, material (e.g., contracts, offer letters, job specifications) used in visa applications and attachments, notes and other contemporaneous documents regarding visa applications and attachments; and discarded material evidencing false documents and information in visa applications and attachments;

b. Files, records, and other items relating to employees, including but not limited to offers of employment, employment contracts, Security Deposit Agreements, Master Services Agreements, Statements of Work, resumes, wage or salary information, employment offers, travel documents, identification documents, records relating to dates of retention and termination; and discarded material evidencing false documents and information with regard to employment or contracting relationships;

c. Files, records, and other items relating to the marketing of employees, including but not limited to marketing materials, memoranda regarding employees, staffing calendars, worker schedules, timesheets, attendance records, interview schedules, requests for specialized labor from prospective clients;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Files, records, and other items relating to financial transfers with foreign-national employees and/or clients or vendors with which those employees were placed, including records showing the wiring or transfer of money or currency from copies of checks and/or actual wire transfer instructions, wire receipts, and/or bank account records showing the wiring or transfer of money via check or wire.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EXHIBIT A

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, RICHARD LIN, a Special Agent with the Diplomatic Security Service (DSS) in San Francisco, California, having been duly sworn, state as follows:

AFFIANT BACKGROUND

1. I am a Special Agent of the Diplomatic Security Service (DSS), which is an agency of the United States State Department, and I have been so employed for over 15 years. I am presently assigned to the Document and Benefit Fraud Task Force at the United States Department of Homeland Security (DHS). This task force investigates sophisticated immigration frauds. In the context of my work for this task force, I have received and continue to receive specialized training and instruction from State Department officers who issue entry visas to foreigners overseas and DHS officers who issue employment documents to foreigners already inside of the United States. I am empowered under 22 U.S.C. § 2709 to investigate visa frauds, as well as to apply for and serve federal arrest and search warrants. My previous assignments include postings in New York, Washington, D.C., Los Angeles, Karachi, Pakistan, and Beirut, Lebanon, as well as numerous long-term temporary-duty assignments throughout the Middle East and South Central Asia. Prior to DSS, I served in the U.S. Marine Corps Reserve. I also have a Master's Degree in Public Administration from the University of Georgia.

INTRODUCTION AND PURPOSE OF AFFIDAVIT

2. This Affidavit is submitted in support of an application for warrants to search the following locations for evidence of violations of Title 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1546(s) (visa fraud), and 18 U.S.C. §

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1341 (mail fraud) (collectively the "Specified Federal Offenses"). The locations set out below are referred to collectively as the "SUBJECT LOCATIONS." The SUBJECT LOCATIONS are described in additional detail in Attachments A-1 and A-2 to this Affidavit and Application, which are attached hereto and incorporated by this reference:

a. **Offices of Azimetry, Inc., located at 14320 NE 21st St., Suite 14, Bellevue, WA 98007 (hereinafter "SUBJECT LOCATION 1").** SUBJECT LOCATION 1 is described in additional detail in Attachment A-1, which is attached hereto and incorporated by this reference. On April 18, 2017, I reviewed records maintained by the Secretary of State for Washington State, which show that Azimetry, Inc. ("Azimetry") is an active corporation that was incorporated in the State of Washington and is located at 14320 NE 21st Street, Suite 14 in Bellevue, Washington. Those records also identified Azimetry's "Governing Persons" as Pradyumna K. Samal ("PK Samal") and Rory O'Flaherty ("O'Flaherty"). Other DHS agents and I have confirmed that Azimetry operates out of the above-listed address in a number of ways, including by reviewing the address set forth on H-1B visa applications submitted by Azimetry,[1] conducting in-person surveillance outside the location,[2] and conducting an in-person site-visit at the address on May 31, 2017, during which I met with Samal (Azimetry's Chief Executive Officer) and confirmed that Azimetry operates out of this address.

b. **Offices of Divensi, Inc. (A/K/A Divensi Technology, Inc.), located at 14320 NE 21st St. Suite 11, Bellevue, WA 98007 (hereinafter "SUBJECT LOCATION 2").** SUBJECT LOCATION 2 is described in additional detail in Attachment A-2, which is attached hereto and incorporated by this reference. On April 18, 2017, I reviewed records maintained by the Secretary of State for Washington State, which show that Divensi, Inc. ("Divensi") is an active corporation that is incorporated in

---

[1] H1-B visas and the process for applying for such visas are described below.

[2] Law enforcement agents conducted in-person surveillance outside Subject Location 1 on September 12, 2017, and confirmed that Azimetry continues to operate there.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the State of Washington and is located at 14320 NE 21st St. Suite 11, Bellevue, WA 98007. These records also identified Divensi's "Governing Persons" as PK Samal and O'Flaherty. Other DHS agents and I have confirmed the Divensi operates out of the above-listed address in a number of ways, including through in-person surveillance,[3] and an in-person site-visit at the address on May 31, 2017, during which I met with Samal (Divensi's CEO) and confirmed that Divensi operates out of this address.

3. Based on my training, experience, and investigation to date, I believe that fruits, instrumentalities, and evidence of violations of the Specified Federal Offenses, as described in this application and affidavit will be found at the SUBJECT LOCATIONS. The items to be seized are described in Attachment B. I request that the search warrants authorize the search of all of the rooms, attics, basements, and all other parts therein, whether locked or unlocked, and surrounding grounds, garages, storage rooms, and outbuildings of any kind, attached or unattached, locked or unlocked, located at the SUBJECT LOCATIONS. Moreover, as set out below, there is probable cause to believe that the items listed in Attachment B are contained in certain computers and other electronic devices, including electronic-storage devices (collectively "digital devices"), at the SUBJECT LOCATIONS. I therefore request the authority to conduct a search of digital devices at the SUBJECT LOCATION, and to seize from those devices the items set out in Attachment B, subject to the search techniques described below.

4. The facts set forth in this Affidavit are known to me as a result of my participation in this investigation, from information provided to me by other law enforcement officers and from records, documents, and other evidence obtained during this investigation. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested search warrants, I have not included each and every fact known to me concerning this investigation, but rather those facts which I

---

[3] Law enforcement agents conducted in-person surveillance outside Subject Location 2 on September 12, 2017, and confirmed that Divensi continues to operate there.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

believe are necessary to establish probable cause to search the SUBJECT LOCATIONS. Everything set forth in this Affidavit is true to the best of my knowledge and belief.

STATEMENT OF PROBABLE CAUSE

5. As set out in additional detail below, the SUBJECT COMPANIES provide information-technology services to corporate clients, including a variety of so-called "Fortune 500" companies (and recruiting firms retained by those companies), in the information-technology field. More specifically, at all times relevant to this investigation, the SUBJECT COMPANIES have hired employees with experience in the information-technology field, such as programmers, marketed those employees to corporate clients, and then placed those employees at corporate clients pursuant to contracts entered into between the SUBJECT COMPANIES and their clients (and/or their clients' agents). Many of the employees who the SUBJECT COMPANIES hired and then placed at their corporate clients entered into the United States under specialty-occupation ("H-1B") visas, which the SUBJECT COMPANIES petitioned for in applications filed with the United States Citizenship and Immigration Services (USCIS). In the sub-sections below, I provide additional detail about H-1B visas, including the application process that petitioners like the SUBJECT COMPANIES typically follow when seeking to obtain an H-1B visa for foreign nationals.

6. The sub-sections below also describe the suspected fraud and set forth the probable cause to believe why evidence of that fraud will be found at the SUBJECT LOCATIONS. As explained below, the SUBJECT COMPANIES repeatedly submitted false information to USCIS in applications for H-1B visas, by claiming that the intended foreign-national beneficiaries of those visas already had been assigned to work on projects for two corporate clients named Revel, Inc. ("Revel") and GeoDigital, Inc. ("GeoDigital"). The applications attempted to support these false assertions by using fabricated letters, which were attached to the applications and which purported to have been signed by agents of Revel and GeoDigital. Rather than assign the visa beneficiaries

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to work on projects for Revel and GeoDigital, the SUBJECT COMPANIES marketed (and eventually placed) those employees at other corporate clients.

7. As set out below, at all times relevant to the investigation and continuing into the present, the SUBJECT COMPANIES' core competence has been to recruit and market foreign-national employees in the information-technology field. Through my investigation, I have developed probable cause to believe that the subject fraud has touched upon, and been furthered by, nearly every division and employee at the companies: from the senior executives who interfaced with foreign-national employees and signed fraudulent applications, to the Human Resources employees who compiled petitions, to the marketers who pitched employees to end clients and collected commissions tied to payments made by those clients. To date, Divensi has filed seventy-one visa petitions with DHS for foreign nationals to work on fictitious Revel projects. Azimetry has filed sixty-six visa petitions with DHS for foreign nationals to work on fictitious GeoDigital projects. The most recent such petition was filed in July 2015, but the Government is aware that the SUBJECT COMPANIES continue to correspond and create evidence regarding the employees named in the earlier-filed petitions. The Government has not subpoenaed the SUBJECT COMPANIES for the records set out in Attachment B, though the SUBJECT COMPANIES are aware of the investigation (as explained below).

A. Background Regarding Specialty Occupation ("H-1B") Work Visas

8. The H-1B visa program is a program administered by USCIS. Under the program, employers in the United States may apply to USCIS to issue visas to foreign nationals under which those foreign nationals may enter the United States and work in a "specialty occupation" for the petitioning employer while in this country. In recent years, U.S. employers typically have sought H-1B visas for foreign nationals who have experience and post-graduate degrees in computer programming, biological sciences, and engineering. Because H-1B visas originally were designed to enable U.S. employers to use foreign nationals for certain narrow categories (i.e., "specialty occupation") of jobs in

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the absence of a large enough labor pool in the United States, H-1B visas are subject to strict issuance requirements, including quotas, certifications by the petitioning employers regarding wages, and lengthy processing times.

9. In order to apply for an H-1B visa, a petitioning employer ordinarily must follow all of the following steps:

10. ***First***, the U.S. employer, acting as a petitioner, must submit a Labor Condition Application ("LCA") for Nonimmigrant Workers to the United States Department of Labor ("DOL") through an online portal. In the LCA, the employer must make certain attestations, including that employing a foreign national under an H-1B visa will not adversely affect the working conditions of similarly-situated U.S. workers (e.g., by depressing wages or interfering with a labor strike). The employer must also post a hardcopy or electronic notice of the LCA for ten days at the employer's office and at the offices of the end client (if any) where the foreign worker will work. In the event that DOL approves the LCA and determines that the American company qualifies to hire foreign workers, the petitioning employer is required to maintain the LCA onsite for inspection by immigration and law-enforcement officials. Based on my training and experience, petitioning companies typically save electronic copies of the LCA on their computers or other electronic storage devices and typically will email copies of the LCA and supporting documentation to their employees, government officials upon request, and other companies with which they are engaged in business. Moreover, a copy of the LCA must be given to the H-1B worker no later than when he/she reports to work.

11. ***Second***, if and after the DOL approves a petitioning employer's LCA, the employer must submit to DHS a Petition for a Nonimmigrant Worker (the "I-129" form) for every foreign worker that it wishes to employ pursuant to an H-1B visa. The I-129 is a thirty-six (36) page application that USCIS makes available on its website at www.uscis.gov in a "fillable" portable document format ("PDF"). The form can be completed electronically and then saved to a digital device, after which it can either be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

printed and mailed to DHS or filed electronically.[4] The I-129 requires the petitioning employer to disclose, *inter alia*, the foreign national employee's name and biographical information, the wage that the employer proposes to pay the foreign national, the business address at which the foreign national will work, and information about the employer itself.

12. The I-129 includes numerous sections that require the petitioning employer to certify the truthfulness of the information contained therein and that warn the petitioner about the consequences of including false information in the application.[5] During the application process, DHS informs the petitioner that it reserves the right to verify any information submitted, including through written and telephonic correspondence and "unannounced physical site inspections of residences and places of employment and interviews." Once the I-129 is submitted, DHS adjudicates it based on the information in the application and any supplemental documentation. In the event that DHS approves the I-129, it approves the issuance of an H-1B visa to the foreign beneficiary named in the application, following which the beneficiary may either pick up their visa at an American consulate (if they reside in a foreign country) or may have the visa mailed to them (if they reside in the United States).

13. Some petitioning employers, such as the SUBJECT COMPANIES, are in the business of applying for H-1B visas for employees who ultimately will be assigned to projects for a client of the petitioner's (an "end client"). The petitioning employer acts as an intermediary, by servicing its clients' need for labor to perform specified projects. In

---

[4] In the event that an I-129 is filed electronically, DHS issues an "electronic receipt" – a digital acknowledgment of the filing of an I-129 – to the petitioning employer.

[5] For instance, the I-129 requires the petitioner to "certify under penalty of perjury that this petition and the evidence submitted with it are true and correct to the best of my knowledge." In the accompanying instructions for the I-129, the Petitioner is advised that "[b]y signing this form, you have stated under penalty of perjury (28 U.S.C. section 1746) that all information and documentation submitted with this form is true and correct." The instructions also add that "[i]f you knowingly and willfully falsify or conceal a material fact or submit a false document with your Form I-129, we will deny your Form I-129 and any other immigration benefit. . . . In addition, you will face severe penalties provided by law and may be subject to criminal prosecution." Thus, when a petitioner signs the Form I-129, it assumes the legal responsibility for the truth and accuracy of all information submitted. If an I-129 is not signed, it will not be considered properly filed.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

such visa applications, the petitioning employer demonstrates that the proposed foreign-national beneficiary will be assigned to an end-client project that qualifies as a "specialty occupation" by submitting proof of its commercial relationship with the end client and proof that the foreign-national beneficiary will work on a project for the end client.

14. More specifically, in my experience and training, petitioning employers that seek H-1B visas for employees who will be assigned to the petitioner's end clients typically will submit the following types of documents:

a. **End-client letters** are letters submitted by the petitioner's end client or the third party worksite at which the foreign-national employee will work.[6] The letter generally certifies that the end client has agreed with the petitioning employer that the foreign-national employee will work on a specialty occupation for the end client. In my experience, such letters set forth the name of the foreign-national employee, their future job title, the project(s) to which they will be assigned to, the name of their onsite supervisor, and the projected duration of the foreign-national employee's services for the end client.

b. **Master Service Agreements** ("MSA") between the petitioner, vendor (if any), and the end client are used to clarify and establish the business/contractual relationship(s) between the parties.

c. **Statements of Work** ("SOWs") are contracts between the petitioner, vendor (if any), and end client, and generally serve as contractual extensions to the MSA. SOWs are generally used to specify in greater detail the terms of the end client's project and are sometimes referred to as "Purchase Orders."

d. **Company-support letters** are written by the petitioning company to USCIS on behalf of the foreign worker and identify the foreign worker by name, job

[6] Certain end clients use so-called "trusted vendors" to coordinate their labor needs. In such cases, the "end-client letter" will be submitted by one of those "trusted vendors" and will contain all of the information that an end-client letter generally includes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

duties, education and skills, and establish the contractual relationship(s) between the end client, vendor and any subcontractors.

15. Though DHS does not require petitioning employers to submit such supporting documentation with their applications, in my experience, the absence of such documentation typically will result in USCIS issuing a Request for Evidence ("RFE") to the petitioning employer. Because an RFE can significantly delay the adjudication and issuance of an H-1B visa, petitioning employers ordinarily seek to submit as much supporting documentation as possible with their initial visa applications.

16. The validity date for an H-1B visa is determined by DHS based on the petitioner's alleged dates of employment for the foreign worker/beneficiary. The maximum initial issuance period for an H-1B visa is three years, but can be extended for an additional three years, for a total of six years. In the event that the beneficiary's employment concludes prior to the visa's expiration date, the visa can continue to be used by the beneficiary for subsequent employment, generally so long as notification of the change is made to DHS and DOL.

17. Even if the petitioner acts on behalf of an end client, unless and until the beneficiary's visa has expired or has been transferred to a new petitioning company, the petitioner is the formal employer of the beneficiary. While working at or for the end client, the employee is paid by the petitioner, and it is standard industry practice that the petitioner is paid an ongoing fee by the end client that covers the cost of the wage or salary as well as a profit margin for the petitioner.

B. Background Regarding "Bench-and-Switch" Visa-Fraud Schemes

18. In my training and experience, the H-1B application process sometimes is used to perpetuate fraud, including through the use of false statements in application materials. Petitioning employers typically engage in such schemes in order to gain an unfair competitive advantage in the labor market.

19. I have investigated numerous fraud schemes that commonly are referred to as "bench-and-switch" schemes. In a "bench-and-switch" scheme, a petitioning

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

employer falsely claims to DHS that a foreign-national beneficiary already has been assigned to a project at an end client of the petitioner's. The fraudulent application includes documents that purports to substantiate the foreign-national beneficiary's job assignment at the end client.

20. In reality, the foreign national has not been assigned to work for any such end client, and the purported documents submitted in support of the claim are false and/or doctored. In some cases, the purported end client is a fictitious company that the petitioning employer has created (and, sometimes, conspired with others to create) in order to perpetuate the fraud.

21. In successful "bench-and-switch" schemes, petitioning employers obtain H-1B visas for foreign-national employees through false representations to DHS. Once those visas are granted, or even before the visas are formally approved, the petitioning employer markets the foreign national to end clients other than those named in the actual petition. By doing so, the petitioning employer can shorten (or eliminate entirely) the ordinary lag time between when an end client agrees to use a foreign-national employee and when DHS issues an H-1B visa to that employee. Shortening or eliminating the lag time enables petitioning companies to place employees at end clients faster than their competitors are able to.

C. Facts Establishing Probable Cause

22. As set out above, this investigation arises out of false and fraudulent statements in H-1B applications that the SUBJECT COMPANIES submitted to DHS. On April 29, 2016, the Honorable Brian A. Tsuchida, United States Magistrate Judge for the Western District of Washington, issued a warrant in cause number MJ16-194 authorizing the search of certain email accounts used by Divensi and Azimetry employees (the "email search warrant"). My Affidavit in support of the Application for that warrant is attached hereto as Exhibit A and incorporated by this reference as if fully set forth herein. As explained in Exhibit A, law enforcement officers have reviewed H-1B petitions submitted

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

by Divensi and Azimetry, interviewed foreign-national beneficiaries and end clients, and determined that one or more statements in the petitions were false and/or fabricated.

23. In the paragraphs below, I supplement the facts set out in Exhibit A with additional information that I have learned since April 2016. I also lay out the probable cause to believe that evidence of the Specified Federal Offenses will be found at the SUBJECT LOCATIONS.

24. Since the email search warrant's issuance, I have taken several investigative steps that can be summarized as follows:

a. Review of Publicly Available Records Regarding the SUBJECT COMPANIES: In order to confirm that the SUBJECT COMPANIES have continued to maintain active corporate status in Washington State, I reviewed information about the SUBJECT COMPANIES kept by the Secretary of State for Washington State and on a third-party database named "CLEAR" operated by Thompson Reuters.[7] Those records show that both SUBJECT COMPANIES continue to maintain active corporate status in Washington State. Those records also show that Samal is listed as the CEO and registered agent of SUBJECT COMPANIES and that both SUBJECT COMPANIES maintain their corporate headquarters at the relevant addresses set forth above. Prasad Puvvala is listed as the CFO of both SUBJECT COMPANIES. The records' references to Samal's and Puvvala's positions are consistent with the SUBJECT COMPANIES' I-129 petitions, which likewise identify Samal as the companies' CEO and Puvvala as their CFO.

b. Review of Materials Seized Pursuant to the Email Search Warrant: I have also reviewed the SUBJECT COMPANIES' email files, which were produced and seized pursuant to the email search warrant. The email files illuminate how the SUBJECT COMPANIES prepared fraudulent visa petitions and marketed foreign-national employees to actual end clients. *First*, the email files show that recruiters at the

[7] I reviewed these records on April 19 and April 20, 2017.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUBJECT COMPANIES contacted foreign nationals who were located in the United States or India and convinced those foreign nationals to enter into employment agreements with the SUBJECT COMPANIES, pursuant to which the SUBJECT COMPANIES acquired the right to sell the foreign nationals' expertise to larger end clients. The emails show that almost every member of the recruiting team, assisted by the companies more senior executives, corresponded with foreign nationals with respect to this initial step. *Second*, the email files show that the SUBJECT COMPANIES used in-house human resources employees, as well as an outside consultant,[8] to prepare visa applications. The companies' senior executives, including Samal, regularly reviewed and edited visa petitions prior to filing. *Third*, while visa applications were pending and immediately after they were approved by DHS, the companies' marketers exchanged emails with prospective end clients in which they attempted to place foreign-national employees with those end clients, pursuant to MSAs and SOWs. The companies' marketers took these steps even though the companies' visa petitions asserted (falsely) that the relevant employees already had been assigned to projects for Revel and GeoDigital. *Fourth*, the companies' marketers kept track of their success in placing employees at end clients, and sought commissions from the companies' executives on that basis. Specific examples of such emails are set forth in the sub-sections below. Submitting false visa petitions to USCIS implicated virtually every part of the SUBJECT COMPANIES' regular business affairs.

c. Interviews of Additional H-1B Beneficiaries: As explained in Exhibit A, before applying for the email search warrant, I interviewed several of the foreign-national employees named in the SUBJECT COMPANIES' visa petitions. Since the email search warrant, I have interviewed nine more beneficiaries. Like the

---

[8] The outside consultant was formerly a licensed attorney in Washington State, who was disbarred from the practice of law in Washington State in 1998, and further expelled from the practice of law before DHS in 2005. The outside consultant was not a practicing attorney during the time that he/she prepared visa petitions for the SUBJECT COMPANIES, nor did he/she hold herself out as an attorney in any of the emails that I have reviewed.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

beneficiaries referred to in Exhibit A, these additional interviewees have told me that, notwithstanding the SUBJECT COMPANIES' representations to DHS, they did not work on projects for end clients Revel and GeoDigital (and had no expectation of doing so during the application process). These additional interviewees also have told me that employees at the SUBJECT COMPANIES marketed and/or placed them at end clients other than Revel and GeoDigital.

d. On-Site Interview of Samal on May 31, 2017: On May 31, 2017, I conducted a site visit to the SUBJECT COMPANIES' offices in Bellevue, Washington. During that site visit, I confirmed that the SUBJECT COMPANIES do business at the relevant addresses set out above. I also interviewed Samal in the presence of the SUBJECT COMPANIES' immigration attorney. Samal told me that the SUBJECT COMPANIES' employees consist of employees based in both India and the United States, and that those employees work on projects for end clients as well as internal projects (e.g., recruitment, marketing) for the SUBJECT COMPANIES. Samal also outlined the SUBJECT COMPANIES' corporate structure, which his attorney later described in an email to me. Samal also described the process the SUBJECT COMPANIES' process for preparing visa applications, confirming that during the time period relevant to the investigation, the SUBJECT COMPANIES's own employees prepared visa applications at their place of business.

25. Through these additional investigative steps, I developed probable cause to believe that evidence of the Specified Federal Offenses will be found at the SUBJECT LOCATIONS, including on digital devices found therein. In the sub-sections below, I identify the categories of evidence that I expect to find at the SUBJECT LOCATIONS, as well as the factual basis for my probable cause relating to each such category of evidence.

1. Evidence Relating to Fraudulent Visa Petitions

26. There is probable cause to believe that fraudulent visa petitions, including attachments to those petitions and drafts of those petitions, will be found at the SUBJECT

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

LOCATIONS. In my training and experience, a petitioner for H-1B visas is required to maintain the documentation associated with the visa application process, including the documentation described above, available for public examination at the employer's principal place of business.[9] Specifically, the following documentation is deemed necessary for public examination: (1) the LCA; (2) documentation of wage rate; (3) documentation explaining how actual wage is set; (4) documentation of determining "prevailing wage"; (5) union/employee notification; and (6) a summary of benefits offered to U.S. workers in same occupational classification as H-1B worker, among other documentation. In my experience and training, petitioners store such materials at their places of business beyond the time required by law, in order to address potential future audits by DHS and keep track of foreign-national recruits and employees.

27. There is also probable cause that the SUBJECT COMPANIES' visa applications will be found on digital devices. I have reviewed the petitions that the SUBJECT COMPANIES filed with DHS and determined that the fields in the USCIS forms were completed by the SUBJECT COMPANIES using computers (and were not handwritten). I am also aware that DOL approved labor certifications in emails that DOL sent to the SUBJECT COMPANIES' employees. Moreover, Samal confirmed to me during the May 31, 2017, interview that the SUBJECT COMPANIES used digital devices to complete the application forms. In my training and experience, petitioning employers keep digital copies not only of final drafts of visa applications that they complete electronically, but also of drafts of those applications, which reflect edits made to those applications over time.

28. Indeed, emails produced pursuant to the email search warrant show that employees at the SUBJECT COMPANIES, as well as an outside consultant, circulated

---

[9] *See* 20 C.F.R. § 655.760 (providing that a petitioner "shall make a filed labor condition application and necessary supporting documentation available for public examination at the employer's principal place of business in the U.S. or at the place of employment within one working day after the date on which the labor condition application is filed with DOL.")

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

materials relating to visa applications prior to filing. For instance, on April 17, 2014, a Divensi recruiter emailed Samal regarding a foreign-national employee referred to herein as "B.K.," with the subject header "Client Letter Missing." Samal responded to Singh's email later that day by attaching a copy of a fraudulent letter that purported to have been issued by GeoDigital and which (falsely) claimed that B.K. already had been assigned to a project for GeoDigital. Similarly, on March 19, 2014, an outside consultant emailed Samal and Puvvala regarding the visa application for a foreign-national employee referred to herein as "A.K." In the email, the outside consultant attached the application forms relating to "A.K.," and provided Samal and Puvvala with mailing instructions. The email also attached a fraudulent letter that purported to have been issued by GeoDigital.

29. There is also probable cause to believe that *drafts* of application materials, as well as metadata reflecting edits to those drafts, and the identity of any editors will be found at the SUBJECT LOCATIONS. As set out above, Samal told me on May 31, 2017, that, prior to 2017, the SUBJECT COMPANIES prepared and filed almost all of their visa petitions "in-house" – i.e., using their own employees. Internal emails confirm that Samal and others circulated and edited drafts of visa-application materials, using applications that preserve metadata regarding editing history. For instance:

a. On March 28, 2014, Samal emailed another Divensi employee, and requested a draft copy of a fraudulent letter that purported to have been issued by Revel with regard to a foreign-national employee referred to herein as "M.P.J." After receiving a copy of the letter in a format (".doc") that is compatible with the application Microsoft Word, Samal made edits to the document and recirculated it to the Divensi employee. Divensi thereafter filed with USCIS the version of the letter that incorporated Samal's edits.

b. On April 17, 2014, a Divensi employee emailed Samal regarding a foreign-national employee referred to herein as "B.K.," with the subject header "Client Letter Missing." Samal responded to Singh's email later that day by attaching a copy of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a fraudulent letter that purported to have been issued by GeoDigital and which (falsely) claimed that B.K. already had been assigned to a project for GeoDigital.

c. On March 19, 2014, the SUBJECT COMPANIES' outside consultant emailed Samal and Puvvala regarding the visa application for a foreign-national employee referred to herein as "A.K." In the email, the outside consultant attached the application forms relating to "A.K.," and provided Samal and Puvvala with mailing instructions. The email also attached a fraudulent letter that purported to have been issued by GeoDigital.

2. Evidence Regarding the Recruitment of Foreign-National Employees

30. There is also probable cause to believe that evidence regarding the recruitment of foreign-national employees will be found at the SUBJECT LOCATIONS. Such evidence includes, but is not limited to, lists of recruiting targets, and internal correspondence regarding prospective recruits. It also includes correspondence, contracts, and records of financial transactions between the SUBJECT COMPANIES and foreign-national employees relating to agreements that the companies entered into with the foreign-national employees before filing visa petitions.

31. The SUBJECT COMPANIES routinely recruited foreign nationals and created several documents to evidence the employment relationship. For instance, the SUBJECT COMPANIES' visa petitions attached copies of their employment agreements with the foreign nationals named as beneficiaries in the applications. Internal emails show that employees at the SUBJECT COMPANIES circulated drafts of these employment agreements among themselves and with the foreign-national beneficiaries during the recruitment process (and before those contracts later were signed and sent to USCIS). For instance, in an email exchange between February and March 2015, a Divensi employee instructed a foreign-national employee named "S.D." to sign an "offer letter" that was sent to the employee in electronic form. After Divensi and the employee

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

negotiated over the terms of the offer letter (e.g., compensation), the employee promised to sign the letter "and send over to" Divensi.

32. Other email exchanges, such as a May 2014 email exchange between various Divensi employees, including Samal, and a foreign-national employee referred to herein as "A.M.," show that Divensi sometimes signed offer letters, and then scanned and emailed the letters to employees with instructions for them to countersign.

33. The SUBJECT COMPANIES also routinely required foreign-national employees to enter into so-called "Security Deposit Agreements," through which the companies effectively shifted visa fees to employees. Foreign-national employees informed me about the Security Deposit Agreements during interviews and showed me copies of the agreements. The agreements required the employees to pay the SUBJECT COMPANIES an up-front fee that approximated the visa-application fee that the SUBJECT COMPANIES eventually paid. For instance:

a. In a January 2015 email exchange, a Divensi recruiter directed a foreign-national employee referred to herein as "S.R." to sign and return a Security Deposit Agreement, which the recruiter attached to the email in digital form. The recruiter also directed S.R. to wire funds to a Divensi bank account in the United States (and to a bank account in Samal's name in India). After S.R. sent an initial payment, the recruiter sent an email stating, "We have received your first payment."

b. In late March 2014, the SUBJECT COMPANIES recruited a foreign-national employee referred to herein as "R.V." On March 26, 2014, R.V. sent an email to her Divensi recruiter, in which R.V. confirmed that R.V. "transferred remaining $2600 through wire transfer. Please find the money transfer receipt." In internal Divensi emails, the recruiter corresponded with the SUBJECT COMPANIES' executives, in order to confirm that the wire transfer had taken place.

c. In March 2014, the SUBJECT COMPANIES recruited a foreign-national employee referred to herein as "L.N." Before preparing and filing a visa petition relating to L.N., the SUBJECT COMPANIES' recruiter directed L.N. to provide Divensi

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

with a copy of L.N.'s resume, and to wire a security deposit to a bank account controlled by Divensi. In accordance with these instructions, L.N. wired money to Divensi's bank account.

34. As with the employment agreements between the SUBJECT COMPANIES and foreign-national employees, I believe there is probable cause that copies of the Security Deposit Agreements and evidence of financial transfers between employees and the SUBJECT COMPANIES will be found at the SUBJECT LOCATIONS. Interviews and internal emails indicate that numerous company recruiters sent the same Security Deposit Agreements to foreign-national employees, which suggests the existence of a central digital template (or templates), which recruiters accessed, modified, and transmitted. Moreover, because the Security Deposit Agreement requires signatures from both parties to the agreement, I believe there is probable cause that hard copies of the agreements will be found at the SUBJECT LOCATIONS. It is also my experience that recruiting companies, like the SUBJECT COMPANIES, will keep central digital records, such as spreadsheets, that reflect financial transfers between foreign-national employees and those companies.

35. There is also probable cause to believe that documents reflecting the relationship between the SUBJECT COMPANIES' competitors (i.e., other recruiting companies) and foreign-national employees will be found at the SUBJECT LOCATIONS. In some cases, the SUBJECT COMPANIES recruited foreign-national employees who already resided and worked in the United States for existing end clients. For instance, during an interview in or about November 2016, a foreign-national employee referred to herein as "S.E." told me that Divensi recruited him in early 2014, while he was already employed by a placement firm named Tata Consultancy Services for a project at end-client Microsoft. Internal Divensi emails show that Divensi's recruiters and executives understood, during the visa-application process relating to S.E., that S.E. already worked for Microsoft and would continue to do so after he moved to Divensi from Tata Consultancy Services. For instance, a September 18, 2014, email

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

from a Divensi recruiter to Samal and others referred to S.E. as a "New Hire-Direct Microsoft" and discussed S.E.'s pay rate. Approximately one month later, S.E. informed a Divensi recruiter about his position at Microsoft and the name of his manager, and the recruiter immediately forwarded the email to Samal with the note "FYI."

3. Evidence Regarding the Marketing of Foreign-National Employees

36. There is also probable cause to believe that evidence regarding the marketing of foreign-national employees to end clients (and/or end clients' vendors) will be found at the SUBJECT LOCATIONS.

37. In my training and experience, petitioning employers regularly maintain personnel files for employees in hard copy and/or digital format at their offices. Such personnel files include materials regarding the marketing of such employees to end clients, including but not limited to contracts with end clients, purchase orders, and correspondence with end clients about employee performance. I am also aware that petitioning employers regularly maintain records relating to financial transfers from end clients, which can show the revenues that petitioning employers earned by marketing foreign-national employees to end clients. In the context of a bench-and-switch scheme, such evidence can show that the petitioning employer marketed a foreign-national employee to end clients other than those named in the petition, thus demonstrating the falsity of the petition.

38. Internal emails show that, after entering into agreements with foreign-national employees, the SUBJECT COMPANIES' marketers marketed the employees to end clients and their agents, notwithstanding representations in the visa petitions about the employees' purported work on projects for Revel and GeoDigital. Because marketing employees and collecting fees from end clients represented the core of the SUBJECT COMPANIES' business, evidence of marketing activity is extensive. Indeed, emails and other materials produced by end clients show that many of the end clients to whom the SUBJECT COMPANIES directed foreign-national employees were located thousands of miles away from the SUBJECT LOCATIONS, giving rise to probable cause that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

negotiations and other correspondence between the SUBJECT COMPANIES and those clients took place electronically and through the exchange of documents, rather than in person.

39. Email correspondence between the SUBJECT COMPANIES' marketers and end clients makes clear that end clients routinely sent MSAs and SOWs, in both draft and final form, to the SUBJECT COMPANIES. In my experience and training, both MSAs and SOWs routinely require signatures from the contracting parties, which gives rise to probable cause that drafts and final versions of those agreements will be found at the SUBJECT LOCATIONS. The SUBJECT COMPANIES' emails also show that marketers at the companies regularly corresponded with employees and end clients, by forwarding employees' resumes to end clients, negotiating salaries and other terms of employment, and arranging interview schedules.

40. Such correspondence, between marketers and end clients, is evidence that representations in the visa petitions regarding purported projects for Revel and GeoDigital were false. For instance, Divensi's recruiters communicated with end clients on behalf of a foreign-national employee referred to herein as "M.R.," even though the relevant visa petition asserted (falsely) that M.R. would be assigned to a project for Revel. On November 17, 2014, approximately two weeks after the U.S. Consulate issued M.R. a visa foil, a Divensi recruiter emailed a potential corporate client named Akvelon. The email referred to M.R. as a "Strong SDE," which in my experience and training is an acronym for "Software Development Engineer." The body of the email attached M.R.'s resume and stated, "Hi Stacy, Please find attached one .net SDE resume. He is a pretty strong developer with C# and SQL. He is available for skype interview." An email sent from a third-party recruiting company to a Gmail account in M.R.'s name listed a variety of available positions throughout Northern California. When I asked M.R. if he had any knowledge of the Gmail address in his name, he claimed that he did not, and speculated that someone at Divensi must have created it in order to market him to end clients. M.R. also told me that, soon after USCIS approved his visa, Puvvala told him that the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

purported Revel project had been cancelled and that Divensi was in the process of marketing M.R. to other end clients.

41. Other email exchanges, such as the examples below, establish probable cause to believe that the SUBJECT COMPANIES marketed and placed foreign-national employees at end clients other than those referenced in the relevant visa petitions:

a. During the first three weeks of September 2014 various vendors and end clients communicated with a foreign-national employee referred to herein as "R.V.," as well as the Divensi marketer assigned to market R.V. to end clients. After vendors emailed R.V. on September 12 and September 18, 2014, regarding potential positions at end clients, a Divensi recruiter responded to each vendor, claiming to be the "representative for Divensi working with [R.V.] who is available for corp to corp." The recruiter also claimed that "[w]e currently hold [R.V.'s] visa" and inquired about the ability to place R.V. with end clients on a "corp to corp" basis. Notwithstanding the recruiter's efforts to place R.V. with end clients in September 2014, R.V.'s visa petition, which was not even approved until October 1, 2014, claimed that R.V. already had been assigned to a project for GeoDigital. During an October 20, 2016 interview, R.V. told me that, during the visa-application process, the Divensi marketer told her that that there was no job for her and that she should try to find her own job.

b. In February 2015, a recruiter at the SUBJECT COMPANIES attempted to market a foreign-national employee referred to herein as "L.N." to two IT vendors in the Seattle area, even though the Azimetry told DHS in an April 2014 visa petition that L.N. already had been assigned to a project for GeoDigital. Indeed, when I interviewed L.N. on January 31, 2017, he told me that after his visa was approved, he was benched without pay from approximately February 2015 to April 2015. While benched, L.N. searched for end clients on his own. I have reviewed two emails, which were sent by L.N. to the SUBJECT COMPANIES' marketers on May 19, 2014, and Samal on March 16, 2015, in which L.N. requested assistance regarding the job search. In the latter email, L.N. asked for the opportunity to meet Samal at Samal's office.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. On February 24, 2015, a marketer emailed Samal and other executives to inform them that a foreign-national beneficiary referred to herein as "R.C." had worked for an end client named Merit Staffing since February 18, 2015, even though Divensi claimed in an April 2014 petition that the same employee would work for Revel once granted entry to the United States.

d. On October 9, 2014, a foreign-national employee referred to herein as "S.S." sent an email to a marketer, in which he told the marketer that he already was working for end client FedEx Corporation in Tennessee. The marketer forwarded the email to Samal the same day.

42. Other internal emails show that the SUBJECT COMPANIES' marketers regularly kept track of their combined efforts to market foreign-national employees in spreadsheets and emails. For instance, in an October 9, 2013, email to Samal and other executives, a marketer embedded a spreadsheet which set forth job placements for various foreign-national employees, including an employee referred to herein as "M.P." The spreadsheet stated that M.P. was assigned to a project for end client Microsoft, despite Samal's claim in an April 9, 2013, visa petition that M.P. would be assigned to a project for Revel at Divensi's Bellevue offices.[10] The spreadsheet referred to other employees' placements at end clients other than Revel, notwithstanding contrary claims in the relevant visa petitions filed by the SUBJECT COMPANIES. Because the spreadsheet appeared to refer to foreign-national employees assigned to marketers other than the email's sender, there is probable cause to believe that marketers had access to a central repository of information regarding job placements (e.g., a shared spreadsheet stored on company servers or circulated over email). Indeed, other company emails show that *both* marketers *and* executives kept track of job placements in order to calculate the marketers' commissions.

[10] The spreadsheet also referred to other foreign-national employees whose petitions claimed that they would be assigned to work for Revel. The spreadsheet stated that those foreign-national employees were, in fact, assigned to projects for end clients other than Revel.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. Evidence Regarding Payments from Actual End Clients

43. There is also probable cause to believe that the SUBJECT LOCATIONS will contain evidence regarding the commercial relationships between the SUBJECT COMPANIES and the actual end clients at which foreign-national employees worked. In my training and experience, petitioning employers regularly keep records relating to financial transactions with end clients (and end clients' vendors), such as timesheets, invoices, checks, and records of commissions. As set out in Exhibit A, the SUBJECT COMPANIES operated email addresses whose sole purpose was to collect information about the time that foreign-national employees spent at end-client worksites. I have reviewed emails that reflect timekeeping records for employees, and which make clear that the SUBJECT COMPANIES regularly kept track of such information in the course of their business.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

44. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT LOCATIONS, in whatever form they are found. One form in which the evidence, fruits, and/or instrumentalities might be found is data stored on digital devices. "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players, such as computer hard drives or other electronic storage media. Electronic Storage media is any physical object upon which

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

45. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

46. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that there is probable cause to believe that digital devices and other electronic storage media at the SUBJECT LOCATIONS contain evidence of the Specified Federal Offenses, and have been used as instrumentalities of those offenses. For the reasons explained above, there is probable cause to believe that the SUBJECT COMPANIES' executives, recruiters, marketers, and human-resources professionals used digital devices to perpetuate the fraud, thereby collecting extensive evidence of the Specified Federal Offenses.

47. There is probable cause to believe that digital devices at the SUBJECT LOCATIONS that have access to the companies' files and email servers have been used to prepare false visa petitions, file false petitions, correspond with foreign-national employees, and market those employees to end clients. In this regard, *digital devices at the SUBJECT LOCATIONS that have access to the SUBJECT COMPANIES' servers and/or files are instrumentalities of the Specified Federal Offenses and are permeated with fraud.* In my training and experience, petitioners, like the SUBJECT COMPANIES, maintain records, such as the submission and receipt of the LCA and I-129 described above on computers and external hard drives/storage devices. There is also probable cause to believe that email messages and other files, such as notes and other correspondence will evidence the process by which the SUBJECT COMPANIES prepared false petitions, including information about who directed and instructed the preparation those petitions.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

48. Indeed, a site plan provided to me at the May 31, 2017 site visit to the SUBJECT LOCATIONS designates one of the rooms in the building as "Computer." In my training and experience, the use of the term "Computer" to refer to a room in a business often indicates the presence of a server. I am also aware that servers act as central repositories of data in businesses, and enable a business' employees to access, edit, and share common files from their local workstations.

49. There is, therefore, probable cause to believe that evidence of the Specified Federal Offenses exists and will be found on digital devices or other electronic storage media at the SUBJECT LOCATIONS, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

50. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the Specified Federal Offenses, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on digital devices or other electronic storage media located at the SUBJECT LOCATIONS because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

51. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements.* Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

52. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

53. Numerous employees work at the SUBJECT LOCATIONS. Given the nature of the SUBJECT COMPANIES' business, it is likely that most, if not all, of those employees will be in possession of digital devices at the time of the search. As explained above, however, the fraud under investigation touched upon virtually every aspect of the SUBJECT COMPANIES' business, and there is probable cause to believe that every division (and every employee within every division) of the company possesses digital evidence of the Specified Federal Offenses. Notwithstanding the fact that all of the digital devices that are used for business purposes are likely to possess such evidence, I expect that some employees may also be in possession of digital devices that are solely intended for their personal use. In the event that law enforcement officers determine, based upon statements by employees or otherwise, that a digital device has been used solely for personal use, they will not seize or search it.

54. In addition, as explained above, the SUBJECT COMPANIES conduct legitimate business, by providing information-technology services and labor to end clients. The seizure of the SUBJECT COMPANIES' digital devices may limit their ability to conduct any such legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If the SUBJECT COMPANIES so request, the agents will, to the extent practicable, attempt to provide the SUBJECT COMPANIES with copies of data that may be necessary or important to the continuing function of their legitimate business, if any. If, after inspecting the computers, it is determined that some

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

55. Finally, as explained above, the SUBJECT COMPANIES have retained immigration counsel, within the last year, to assist with petitions. The Government is also aware that the SUBJECT COMPANIES have retained counsel to assist with this investigation. As a result, there may be attorney-client privileged material among the records sought by the application. In order to prevent inadvertent exposure to such material by those individuals involved in this investigation, the search of the SUBJECT LOCATIONS and the initial seizure of authorized records, computer and digital devices will be wholly conducted by law enforcement agents who, after the search and seizure, will have no further role in the investigation of this matter, other than to establish chain of custody and, if needed, to provide information and/or testimony regarding the conduct of this search and seizure. The search and seizure team will be advised as to the identities of all relevant counsel and will be instructed to avoid review of any material that may constitute attorney-client communication or attorney work product, never communicate to members of the investigative team the contents of such suspected privileged material, and seize only material authorized by this warrant.

56. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.[1]

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site

---

[1] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

Searching the Forensic Images

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

REQUEST FOR SEALING

57. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, affidavit and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation and disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Disclosure of these materials would give the target of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

58. Based on the foregoing, there is probable cause that the Subject Companies have committed violations of 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1546(a) (visa fraud), and 18 U.S.C. § 1341 (mail fraud). I request the issuance of search warrants authorizing the search of the SUBJECT LOCATIONS for evidence, instrumentalities, and fruits of the Specified Federal Offenses and the seizure of those items whether in electronic or non-electronic form.

Richard Lin, Affiant
Special Agent
Diplomatic Security Service
U.S. Department of State

Subscribed to before me this 29 day of September, 2017.

MARY ALICE THEILER
United States Magistrate Judge

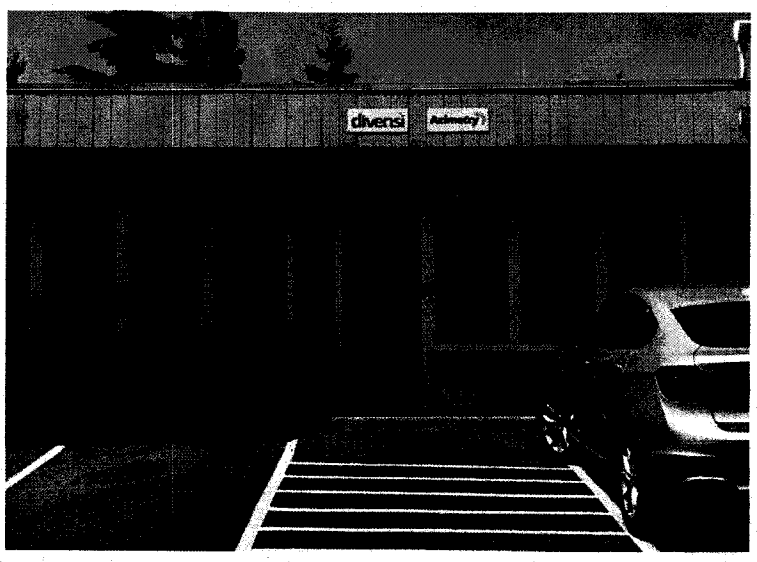
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

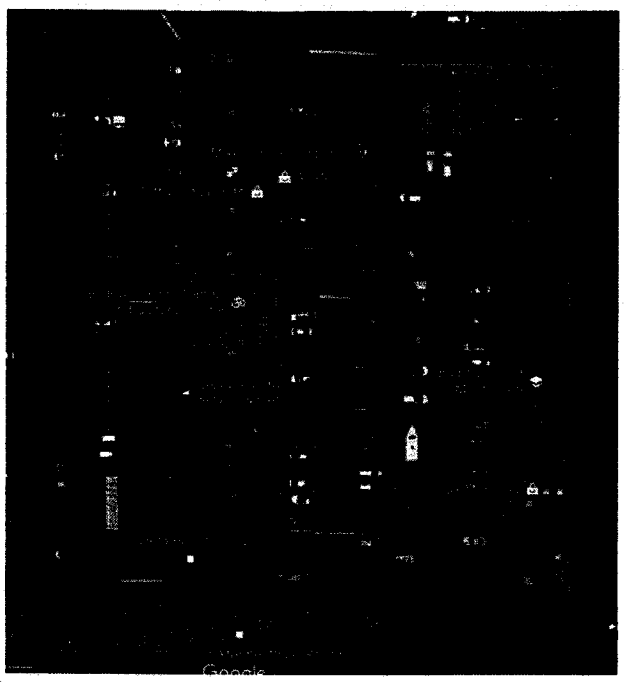
Description of Property to be Searched

Azimetry, Inc. is located at 14320 NE 21st St. Suite 14, Bellevue, WA 98007 in a single story building in a mixed-use office park off NE 21st St.

Front Door



Satellite View



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

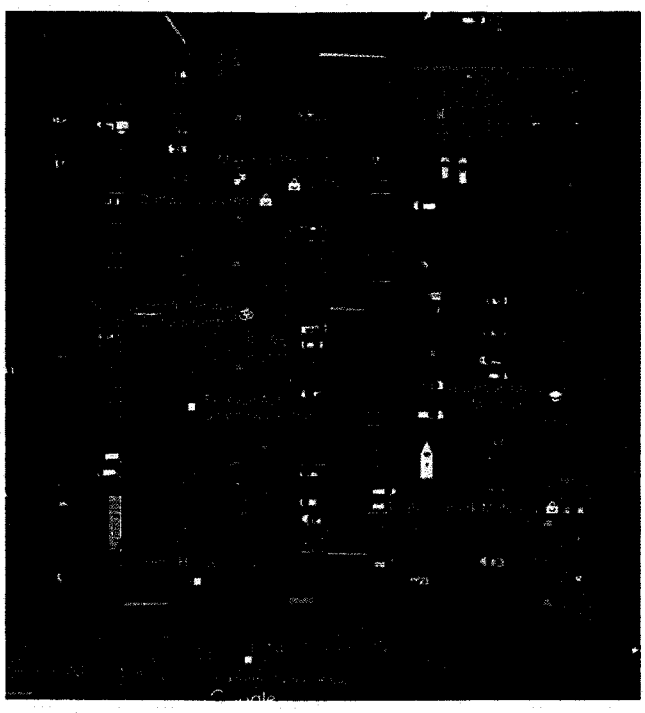
ATTACHMENT A-2

Description of Property to be Searched

Divensi, Inc. is located at 14320 NE 21st St. Suite 11, Bellevue, WA 98007 in a single story building in a mixed-use office park off NE 21st St.

Front Door

Satellite View



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Items to Be Seized

The items to be seized are the following items or materials[11] that may contain evidence of the commission of, the fruits of, or property which has been used as the means of committing, federal criminal violations of Title 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1028A (aggravated identity theft), 18 U.S.C. § 1546(s) (visa fraud), 18 U.S.C. § 1028A (aggravate identity theft) and 18 U.S.C. § 1341 (mail fraud), for the period 2012 to the present:

a. Evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1546(s) (visa fraud), 18 U.S.C. § 1028A (aggravate identity theft) and 18 U.S.C. § 1341 (mail fraud).

b. Files, records, and other items showing residency and/or dominion and control of the places to be searched, including but not limited to keys, receipts, bills, canceled checks, mail envelopes, rental agreements, telephone records and bills, utility bills, and internet/cable provider statements;

c. Files, records, and other items relating to applications for visas and other forms of legal status in the United States, including but not limited to, visa applications and attachments, drafts of visa applications and attachments,[12] information regarding the preparation of visa applications and attachments, correspondence relating to visa applications and attachments, material (e.g., contracts, offer letters, job specifications) used in visa applications and attachments, notes and other contemporaneous documents

---

[11] As used in this Attachment, the term "records" includes all of the items described in whatever form and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, paper, digital, and/or magnetic forms. It also includes items in the form of computer hardware, smart phones, software, documentation, passwords, e-mail, and/or data security devices.

[12] Because the last petition relating to Revel or GeoDigital was filed in July 2015, the Government only seeks authority to seize actual applications and drafts of applications that were filed between 2012 and July 2015. The Government nevertheless seeks authority to seize the other application-related materials (such as correspondence) beyond the July 2015 date, because the Government has reason to believe that the SUBJECT COMPANIES continued to market foreign-national employees after that date.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

regarding visa applications and attachments; and discarded material evidencing false documents and information in visa applications and attachments;

d. Files, records, and other items relating to employees, including but not limited to offers of employment, employment contracts, Security Deposit Agreements, Master Services Agreements, Statements of Work, resumes, wage or salary information, employment offers, travel documents, identification documents, records relating to dates of retention and termination; and discarded material evidencing false documents and information with regard to employment or contracting relationships;

e. Files, records, and other items relating to the marketing of employees, including but not limited to marketing materials, memoranda regarding employees, staffing calendars, worker schedules, timesheets, attendance records, interview schedules, requests for specialized labor from prospective clients;

f. Files, records, and other items relating to financial transfers with foreign-national employees and/or clients or vendors with which those employees were placed, including records showing the wiring or transfer of money or currency from copies of checks and/or actual wire transfer instructions, wire receipts, and/or bank account records showing the wiring or transfer of money via check or wire.

g. Any computer equipment or digital devices that are capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, including central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices including paging devices and cellular telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communication devices such as modems, routers, cables, and connections; storage media; and security devices. The authority to seize

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer equipment or digital devices includes the authority to search the following computer equipment or digital devices for the items set out in the preceding paragraphs[13]:

i. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes referenced above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes;

ii. Any magnetic, electronic, or optical storage device capable of storing data, such as flash drives, floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes referenced above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes;

iii. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

iv. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

v. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

vi. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

---

[13] As set out in the Affidavit, the law enforcement agents who execute the search warrant will make every effort to determine, through statements by employees and otherwise, whether particular digital devices are solely for personal use and have not been used to access the SUBJECT COMPANIES' files and/or servers. In the event that such devices are determined to be for purely personal use, law enforcement officers will not seize and search them.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

vii. All records, documents, programs, applications, or materials that show the actual user(s) of the computers or digital devices during the time the device was used to commit the crimes referenced above.

h. Records showing the subscriber or account holder of any IP addresses and records showing the subscriber or account holder of any wireless internet access devices.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EXHIBIT A

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

STATE OF WASHINGTON ss

COUNTY OF KING

I, Richard Lin, being duly sworn, depose and state as follows:

I. INTRODUCTION AND AFFIANT BACKGROUND

1. I make this Affidavit in support of an application for search warrants authorizing the examination of the following email accounts (collectively, the "Subject Email Accounts"):

pksamal@divensi.com;
prasadp@divensi.com;
larryw@divensi.com;
roryo@divensi.com;
mansin@divensi.com;
komals@divensi.com;
timecard@divensi.com;
bhartig@divensi.com;
ajayd@divensi.com;
mayanks@divensi.com;
hubbelo@divensi.com;
pksamal@azimetry.com

2. The domain names divensi.com and azimetry.com are owned and operated by webhost and email service provider Go Daddy, located at 14455 N. Hayden Rd. Suite 219, Scottsdale, AZ 85260. The information to be searched is described in the following paragraphs and in **Attachment A**, and is stored at a premises controlled by Go Daddy. This Affidavit is made in support of an application for a search warrant under 18 U.S.C.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

§§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Go Daddy to disclose to the government copies of the information (including the content of communications) further described in Section I of **Attachment B**. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. On November 20, 2015, I issued Go Daddy a preservation letter requesting that all e-mails and associated files for the domain names @divensi.com and @azimetry.com be saved for 90 days, and on November 30, 2015 Go Daddy responded informing me that the order had been received and emails @divensi.com and @azimetry.com would be preserved. On February 18, 2016, I issued Go Daddy another preservation letter asking that all e-mails and associated files for the domain names @divensi.com and @azimetry.com be saved for another 90 days.

3. Based on my investigation, information I have received from employees of Divensi, Inc., and Azimetry, Inc. (hereinafter "Subject Companies") and documents submitted to the U.S. government by Subject Companies, the aforementioned email addresses are owned and operated by SAMAL, Pradyumana Kumar (hereinafter "SAMAL") and corporate officers and employees of SAMAL's company Divensi, Inc., located at 14320 NE 21st St. Suite 11, Bellevue, WA 98005 and Azimetry, Inc., located at 14320 NE 21st St. Suite 14, Bellevue, WA 98005. Information that I have collected in the course of this investigation establishes probable cause to believe that within the contents of the Subject Email Accounts there exists evidence, fruits and/or instrumentalities of violations of 18 U.S.C. § 1001 (False Statements); 18 U.S.C. § 1546 (Visa Fraud); and 18 U.S.C. § 371 (Conspiracy). Information that I have collected in the course of this investigation also establishes probable cause to believe that SAMAL, Prasad PUVVALA, Ajay DOHRAY and Komal SINGH have violated the federal laws set out above.

4. In sum, Subject Companies provide information technology services to various Fortune 500 and other corporate clients, largely by obtaining specialty occupation ("H-1B") work visas for and placing high-technology workers from India at the corporate

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

clients. Subject Companies through their corporate officer SAMAL, and others, have been fraudulently obtaining some or all of these H-1B work visas from the Department of Homeland Security ("DHS"). The fraudulent scheme entails the submission of false documentation in support of the H-1B work visa petitions to DHS. Specifically, Subject Companies have submitted, in support of H-1B work visa petitions, documentation that was purportedly issued by Revel, Inc. and GeoDigital, Inc. and which purported to state that the visa recipients would be assigned to work on projects for Revel, Inc. and/or GeoDigital, Inc. In truth, no such documentation had ever been issued by Revel, Inc. and GeoDigital, Inc. and the Subject Companies had never been authorized to issue any such documentation in the name Revel, Inc. and/or GeoDigital, Inc. To date, Divensi, Inc. has filed 71 H-1B visa petitions to DHS for foreign workers to work on Revel, Inc. projects while Azimetry, Inc. has filed 66 H-1B visa petitions to DHS for foreign workers to work on GeoDigital, Inc. projects for a total of 137 suspected fraudulent visa petitions.

5. The facts set forth in this Affidavit are known to me as a result of my participation in this investigation, from information provided to me by other law enforcement officers and from records, documents, and other evidence obtained during this investigation. Since this Affidavit is being submitted for the limited purpose of establishing probable cause for the requested search warrants, I have not included each and every fact known to me concerning this investigation, but rather those facts which I believe are necessary to establish probable cause to search information associated with the Subject Email Accounts. Everything set forth in this Affidavit is true to the best of my knowledge and belief.

II. AFFIANT BACKGROUND

6. I am a Special Agent of the Diplomatic Security Service ("DSS"), which is an agency of the United States Department of State ("State Department"), and I have been so employed for over 14 years. I am presently assigned to the Document and Benefit Fraud Task Force at DHS. This task force investigates sophisticated immigration frauds in the San Francisco Bay Area, and as such, I have received and continue to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

receive specialized training and instruction from State Department officers who issue entry visas to foreigners overseas and DHS officers who issue employment documents to foreigners already inside of the United States. I am empowered under 22 U.S.C. § 2709 to investigate visa frauds, as well as to apply for and serve federal arrest and search warrants. My previous assignments with DSS include the New York Field Office, DSS Headquarters, Washington, D.C., U.S. Consulate Karachi, Pakistan, U.S. Embassy Beirut, Lebanon, and the Los Angeles Field Office, along with numerous long-term temporary duty assignments to locales throughout the Middle East and South Central Asia. Prior to DSS, I served in the U.S. Marine Corps Reserve, and I also have a Master's Degree in Public Administration from the University of Georgia's School of Public Policy.

III. BACKGROUND REGARDING SPECIALTY OCCUPATION H-1B WORK VISAS

A. H-1B Work Visa

7. Foreigners wishing to work in the United States must apply for a work visa through DHS, which includes in pertinent part, H-1B specialty occupation work visas. H-1B visas are reserved for specialty occupation foreign workers, namely computer programmers, scientists, and engineers who hold at least a bachelor's degree. H-1B visas were designed so industries could fill skill and labor gaps with foreign workers, and they have strict issuance requirements, lengthy processing times, fees, wage and labor promises, certifications, and quotas.

B. Labor Condition Application (LCA)

8. If a U.S. company wishes to sponsor a foreign specialty occupation worker on an H-1B visa, the U.S. company, acting as a petitioner, begins the process by submitting a Labor Condition Application ("LCA") for Nonimmigrant Workers (ETA Form 9035) to the Department of Labor ("DOL") in Chicago, Illinois. The purpose of the LCA is to ensure that the petitioner has provided qualified American workers sufficient time and opportunity to apply for the proposed job by openly advertising the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

position. Once this obligation is met, the petitioner can then submit the LCA electronically through the iCERT Portal system and will receive a courtesy email confirming receipt of the LCA submission.

9. The DOL then adjudicates the LCA and determines if the American company qualifies to hire foreign workers. If and when the application is approved, the DOL electronically notifies the petitioner and DHS via e-mail. Since Subject Companies utilize a mixture of the email addresses pksamal@divensi.com; pksamal@azimetry.com; and roryo@azimetry.com; on all of THEIR I-129 Petitions (described below) and LCAs, notification would be via these addresses. Once approved, all LCAs are required to be maintained by the petitioner onsite for inspection by immigration and law enforcement officials. Based on my training and experience, petitioning companies typically save electronic copies of the LCA on their computers or other electronic storage devices and typically will email copies of the LCA and supporting documentation to their employees, government officials upon request, and other companies with which they are engaged in business. Moreover, a copy of the LCA must be given to the H-1B worker no later than when he/she reports to work.

10. Based on my investigation and interviews of Subject Companies' foreign workers, as set out below, Subject Companies' Chief Operating Officer (COO) Prasad PUVVALA has emailed LCAs and supporting documentation to H-1B foreign workers from the email address prasadp@divensi.com.

C. The I-129 Petition

11. After the LCA is approved, the petitioner then prepares a Petition for a Nonimmigrant Worker on Form I-129 (herein, "I-129") for every foreign worker they wish to employ and submits the I-129 to a DHS processing center. The I-129 is a 36-page document that is publicly available in a fillable portable document format ("PDF") on the U.S. Citizenship and Immigration Service ("USCIS") website located at www.uscis.gov. This PDF enables the Petitioner to enter data directly onto the form and save it electronically on a computer or other electronic storage device for record keeping

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and printing for submission to DHS. Among other things, the I-129 requires the name and biographical data of the proposed foreign worker, the proposed wage to be paid, and the address where the foreign worker will be working as well as biographical information about the petitioner.

12. The I-129 requires the petitioner to "certify under penalty of perjury that this petition and the evidence submitted with it are true and correct to the best of my knowledge." In the accompanying instructions for the I-129, the Petitioner is advised that "[b]y signing this form, you have stated under penalty of perjury (28 U.S.C. section 1746) that all information and documentation submitted with this form is true and correct." The instructions also add that "[i]f you knowingly and willfully falsify or conceal a material fact or submit a false document with your Form I-129, we will deny your Form I-129 and any other immigration benefit. . . . In addition, you will face severe penalties provided by law and may be subject to criminal prosecution." Thus, when a petitioner signs the Form I-129, it assumes the legal responsibility for the truth and accuracy of all information submitted. If an I-129 is not signed, it will not be considered properly filed.

13. Petitioners have the option to e-file the I-129 with DHS and will receive a receipt indicating the service center to which the I-129 was routed. DHS then reserves the right to verify any information submitted, including through contact via written correspondence, telephone and "unannounced physical site inspections of residences and places of employment and interviews."

14. When the I-129 is submitted to DHS, DHS reviews all of the listed and supplemental documentation and adjudicates it. If qualified, DHS then approves H-1B visa/status to the proposed foreign worker and directs the worker to pick up his/her visa at an American Consulate, or mails them the documentation if they are already in the United States.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

D. End-Client Worksites

15. Some petitioners are in the business of obtaining H-1B visas for employees who will ultimately be placed with or in the service of an end client that has the actual need for the employee. In pertinent part, should such a petitioner, as an intermediary, wish to place their proposed foreign worker at an end-client worksite or on a project on behalf of the end client, the U.S. employer/petitioner can voluntarily submit their contracts, end-client letters, or other documentation along with the I-129s to DHS. Although supporting documentation is not required in the H-1B process, its absence will usually trigger USCIS to issue a Request for Evidence ("RFE"), which can significantly delay the adjudication process. RFEs occur when USCIS is unable to determine eligibility on the evidence provided. In order to avoid delays in processing, most petitioners will submit as much supporting documentation as possible along with the I-129 petition for an H-1B visa.

16. Based on my training and experience, examples of supporting documentation submitted by petitioners include: (1) end-client letters; (2) vendor letters; (3) purchase orders/contracts; (4) Statements of Work; and (5) company-support letters to USCIS.

a. End-client letters are letters submitted by the ultimate client or third-party worksite on behalf of the foreign worker and, in general, include the name of the foreign worker, his/her job title, the project(s) he/she is assigned to, the name of the foreign worker's onsite supervisor, and how long the foreign worker's services will be required.

b. Vendor letters are letters submitted by companies that serve as trusted middlemen between the petitioner and end client on behalf of the foreign worker. Typically, Fortune 500 companies obtain foreign labor through vetted companies known as vendors. In turn, vendors will subcontract their client's requirements to petitioning companies. In general, vendor letters include the name of the foreign worker, his/her job

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

title, the project(s) he/she is assigned to, the name of the foreign worker's onsite supervisor, how long the foreign worker's services will be required and, in addition, describe the contractual relationship between the petitioner, vendor, and end client.

c. Purchase orders/contracts between the petitioner, vendor (if any), and end client are used to clarify and establish the business/contractual relationship(s) between the parties. These documents are sometimes referred to as Master Services Agreements (MSA).

d. Statements of Work (SOW) are contracts between the petitioner, vendor (if any), and end client and are generally extensions of the MSA. SOWs are generally used to specify in greater detail the terms of the end client's project.

e. Company-support letters are written by the petitioning company to USCIS on behalf of the foreign worker and identify the foreign worker by name, job duties, education and skills, and establish the contractual relationship(s) between the end client, vendor and any subcontractors.

17. The validity date for an H-1B visa is determined by DHS based on the petitioner's alleged dates of employment for the foreign worker/beneficiary. The maximum initial issuance period for an H-1B visa is three years, but can be extended for an additional three years, for a total of six years. In the event that the beneficiary's employment concludes prior to the visa's expiration date, the visa can continue to be used by the beneficiary for subsequent employment, generally so long as notification of the change is made to DHS and DOL.

18. Even if the petitioner acts on behalf of an end client, unless and until the beneficiary's visa has expired or has been transferred to a new petitioning company, the petitioner is the formal employer of the beneficiary. While working at or for the end client, the employee is paid by the petitioner, and it is standard industry practice that the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

petitioner is paid an ongoing fee by the end client that covers the cost of the wage or salary as well as a markup for profit for the petitioner.

IV. COMMON H-1B VISA FRAUD SCHEMES

19. Based on my training and experience, I know that H-1B visa fraud schemes generally have recognizable patterns and particular purposes, including, among others;

a. Fraudulent petitioners commonly conspire with others to invent end-client companies from whole cloth. Investigations often reveal that the end client where the beneficiary was petitioned to work does not actually exist.

b. In some cases, the petitioners (and the preparers of the petitions) submit fraudulent materials in support of the petitions, including letters and contracts from the purported end client falsely claiming that the employer has a bona fide employment opportunity for the alien beneficiary.

c. After the petition is approved, fraudulent petitioners profit from the scheme by having a "bench," a supply of qualified H-1B employees, with visas valid for the maximum term, ready to respond immediately to the market needs of actual end clients possessing actual employment offers without the delays or limitations occasioned by the legal process for obtaining legitimate visas. This scheme is commonly referred to as the "bench and switch."

V. BACKGROUND REGARDING INFORMATION TECHNOLOGY IN THIS CASE

20. Go Daddy is a webhost and email service provider. Webhosts enable individuals and organizations to make their website accessible on the World Wide Web (WWW). In addition, webhosts and email service providers also provide their clients/subscribers with a dedicated email domain name and space on their server for the storage of client emails and associated files. Therefore, the computers of Go Daddy are likely to contain stored electronic communications (including retrieved and un-retrieved email for Go Daddy clients/subscribers) and information concerning clients/subscribers

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and their use of Go Daddy services, respectively, such as account access information, email transaction information, and account application information. As mentioned in Paragraph 2 above, I issued a preservation letter to Go Daddy and, as to the initial preservation letter, received confirmation of my request to preserve all emails and files associated with the domain names @divensi.com and @azimetry.com.

21. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

22. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. The internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The internet can also be defined as a worldwide interconnection of computers and computer networks that facilitate the sharing or exchange of information among users. The internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

b. E-mail is a popular form of transmitting messages and files in an electronic environment between computer users. When an individual computer user sends an e-mail message, it is initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

c. Email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location or illicit activities.

d. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service(s) utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

f. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol ("IP") addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

VI. FACTS ESTABLISHING PROBABLE CAUSE

A. Summary of Investigation into Suspected "Bench and Switch" Visa Fraud Scheme by Subject Companies

23. On or about November 19, 2015, I was assigned to investigate Subject Companies due to suspected H-1B visa fraud; specifically the Subject Companies appeared to be filing H1-B petitions for purported job sites and job offers that did not exist. On or about that day, I began my investigation by reviewing the H1-B petitions filed by Subject Companies, including their submitted LCAs, I-129s and supporting documentation, and discovered that many of them contained indications of fraud, namely the hallmarks of what I know to be the "bench and switch" visa fraud scheme. Specifically, SAMAL and O'FLAHERTY, acting on behalf of petitioning companies, Divensi, Inc. and Azimetry, Inc., are doing business at 14320 NE 21st St Suites 11 and 14, Bellevue, WA 98007, and from there have submitted visa petitions and supporting documents claiming that the foreign-worker beneficiaries identified in the petitions would be working onsite at Subject Companies' offices on behalf of projects for end clients Revel, Inc. and GeoDigital, Inc. In actuality, however, the documents submitted by SAMAL and O'FLAHERTY in order to substantiate the existence of those end-client projects were forged and/or altered. As a result of the fraud, DHS has issued numerous

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

H-1B visas to these foreign workers on whose behalf SAMAL and O'FLAHERTY submitted petitions.

24. The petitions submitted by SAMAL and O'FLAHERTY were submitted on behalf of their companies, Divensi, Inc. and Azimetry, Inc. To date, Divensi, Inc. submitted to DHS a total of 71 H-1B visa applications for 67 foreign workers to work on a project on behalf of end client Revel, Inc. while Azimetry submitted a total of 66 H-1B visa applications for 65 foreign workers to work on a project on behalf of GeoDigital, Inc. for a total of 137 suspected fraudulent visa petitions.

B. Investigation into Petitions Submitted by Divensi, Inc.

25. Between on or about September 2015 and on or about February 2016, I performed an investigation in to the H1-B petitions submitted by Divensi, Inc. on behalf of foreign-worker beneficiaries who purportedly were going to work at end client Revel, Inc. My investigation proceeded in two steps. First, I examined the contents and statements in actual H-1B petitions filed by Divensi, Inc. As part of this first step, I approached Revel, Inc. regarding representations about Revel, Inc. that SAMAL and O'FLAHERTY made in the Divensi, Inc. petitions, in order to determine whether those representations were accurate and whether Revel, Inc. had been approached in connection with those representations. Second, I interviewed three of the sixty-seven foreign-worker beneficiaries who Divensi, Inc. identified in its petitions and interviewed them about their experience with Divensi, Inc. and its executives, including SAMAL.

1. Review of Petitions Submitted by Divensi, Inc.

26. On or about January 19, 2016, DSS Investigative Analyst ("IA") David Pinck and I conducted a "Corporations Search" on the Washington State Secretary of State's website and learned that Divensi, Inc. was incorporated in the State of Washington on July 28, 2010. Rory O'FLAHERTY, Divensi, Inc.'s Chief Financial Officer (CFO) is listed as the company's Registered Agent using the address 14320 NE 21st St. Suite 11, Bellevue, WA 98007. On January 19, 2016, I conducted a record check using the database "CP CLEAR" and learned that SAMAL is Divensi, Inc.'s

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

President/Chief Executive Officer (CEO), Himani JAIN is Divensi, Inc.'s Technical Recruiter; Ajay DOHRAY is Divensi, Inc.'s Business Manager; Adam FRANKS is Divensi, Inc.'s Vice-President of Sales and Marketing, and Bharti GUPTA is Divensi, Inc.'s Account Manager. An open source search from the website www.zoominfo.com shows Prasad V. PUVVALA to be Divensi, Inc.'s Chief Operations Officer. The specific url of the webpage that lists PUVVALA as Divensi, Inc.'s Chief Operations Officer is: http://www.zoominfo.com/p/Prasad-Puvvala/1869651214. As explained below, my subsequent investigation has confirmed that PUVVALA has served as Divensi, Inc.'s Chief Operating Officer.

27. From on or about June 2012 to November 2014, SAMAL and O'FLAHERTY, under penalty of perjury, and through their company Divensi, Inc., signed and submitted 71 separate I-129s and supporting documentation on behalf of 67 different foreign-worker beneficiaries to work on an alleged project for Revel, Inc. The supporting documentation in the H-1B work visa petitions that accompanied the I-129s included Revel, Inc. SOWs, LCAs and end client letters attesting that the foreign workers were needed to work onsite at Divensi's office located at 14320 NE 21st St Suite 11, Bellevue, WA 98007 on a project on behalf of Revel, Inc. All of the end client letters were on Revel, Inc. letterhead and contained the alleged signature of Revel, Inc.'s CEO Vikas Kamran.

28. On September 15, 2015, before I was assigned to the case, IA Jeremiah Saylor interviewed Rita Rossing, Revel, Inc.'s Human Resources Generalist. Rossing informed IA Saylor that Revel, Inc. has no record of the 67 beneficiaries petitioned by Divensi, Inc. On or about February 9, 2016, I sent Rossing a DVD containing copies of the 71 Revel end client letters found in the visa petitions of the 67 different worker beneficiaries, all of which were allegedly signed by Revel's CEO Vikas Kamran. On March 7, 2016, after reviewing the 71 end client letters, Rossing informed me that Kamran did not sign any of the letters; that Revel did not authorize Divensi to write any of the letters; and that Revel did not produce any of the letters for Divensi.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

2. Interviews of Foreign-Worker Beneficiaries

a. Interview of Beneficiary A.P.

29. On January 6, 2016, IA Pinck and I interviewed A.P., one of the Divensi, Inc. foreign-worker beneficiaries who had been petitioned by SAMAL to work onsite at Divensi, Inc.'s office, located in Bellevue, WA. The H1-B petition for A.P. has a filing date of April 8, 2013 and an approval date of September 13, 2013. In the petition, SAMAL stated that A.P. would work on an in-house project on behalf of end client Revel. During the interview, A.P. told me that she has never worked at Divensi's office, located in Bellevue, WA or on a project for Revel, a company she had never heard of. A.P. also told me that after her H-1B visa petition was approved, she remained in California where she was benched without pay for approximately two to three weeks while DOHRAY, PUVVALA and JAIN tried to find her projects at end clients other than Revel, Inc.. A.P. said that Divensi, Inc. made her pay approximately $5,000 to file her visa petition.[1]

30. After the interview with A.P., A.P. provided me with email correspondence between herself and Divensi, Inc. employees. In my review of those emails, and through additional investigation, I corroborated A.P.'s statements to me and observed the following evidence of visa fraud:

a. On March 17, 2013, Ajay DOHRAY from ajayd@divensi.com sent an email to A.P. at A.P.'s email address with the Subject heading: "RE: H1B Application" and the message, "Nice talking with you, As discussed, my CEO (PK SAMAL) will call you tonight at 9:30 PM IST to screen you. Meanwhile please fill the details and send me back. Ajay Kumar Dohray Business Development Manager Divensi Inc."

[1] The U.S. Department of Labor's (DOL) website contains a list of rights for H-1B workers. The list states that employers (Petitioners) may not require their workers (Beneficiaries) to pay either directly or indirectly any part of the petition filing fee. The specific website URL for DOL explaining the rights of H-1B workers is http://www.dol.gov/wecanhelp/h1bworkers.htm

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. On March 18, 2013, DOHRAY from ajayd@divensi.com sent an email to A.P.'s husband K.J. with a Carbon Copy (CC) to A.P. containing Divensi, Inc.'s JP Morgan Chase account information and the message "Here are the details for ACH/Wire transfers for Divensi" "Please send me the tracking details…" "Thanks Ajay Kumar Dohray"

c. On March 18, 2013, K.J. sent an email to DOHRAY at ajayd@divensi.com with the message: "Hi Ajay, With your agreement that the starting pay will be $60K, I have scheduled the transfer, below is the confirmation. Also attached is the security deposit form. I will send you the necessary documents tonight. Thanks." Attached to the email was a bank confirmation number showing the amount of $4,750.00 being transferred to Divensi Inc.'s Chase Bank account on March 18, 2013 from K.J. Also attached to the email was a "Security Deposit Agreement" from Divensi, Inc. signed by A.P. on March 18, 2013. In my review of the agreement, I learned that Divensi, Inc. required A.P. to pay $4,750 to process her H-1B visa petition, which is a violation of law.

d. On March 28, 2013, PUVVALA from prasadp@divensi.com sent an email to A.P. with the Subject heading: "FW: Offer Letter Last Page" and the message, "Hi, Please sign this offer letter and send it back this is purely for USCIS application purpose and asusual(sic) you will have your offer letter copy with real negotiated salary plus benefits package with PK [SAMAL] when you really join. This is only for application."[2] Attached to the email was the last page of the A.P.'s Divensi, Inc. offer letter requiring her signature at the bottom.

[2] PUVALLA's email also included his telephone number, which I have omitted for the purpose of maintaining the privacy of that information.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. On March 28, 2013, A.P. sent an email to PUVVALA at prasadp@divensi.com asking him to provide the full offer letter. A.P. wrote "...it doesn't make sense to sign a document without even reading/knowing its contents fully. I'd appreciate if you are more transparent."

f. On March 28, 2013, PUVVALA from prasadp@divensi.com sent an email to A.P. at with the message, "Here is the template that I have for ur review. Accountant has to come and prepare for you full letter and send u.."

g. On July 22, 2013, A.P. from sent an email to PUVVALA at prasadp@divensi.com with the Subject heading: "Re: FW: Updated resume as of today.. Training plans" and the message, "Hi Prasad, I was out of town last week, sorry for the delay. Here is my resume." Attached to the email was a PDF copy of A.P.'s resume.

h. On July 22, 2013, PUVVALA from prasadp@divensi.com sent an email to A.P. with the message, "I need copy in word format in the same template I sent u guys.. Thanks and regards Prasad V. Puvvala COO". During my interview of A.P. A.P. told me that JAIN instructed her to bolster her resume by inserting fake work experience. When A.P. refused, she told me that PUVVALA requested for her to send her the resume in a MS Word format.

i. On September 3, 2013, DOHRAY from ajayd@divensi.com forwarded an email to A.P. with the Subject heading: "Urgent Job Opening: "QA Test Coordinator". Contained in the email was a job opening for an unnamed end client located in San Ramon, CA. The September 3, 2013 email predates the date (September 13, 2014) on which the H1-B petition was approved.

j. On October 2, 2013, DOHRAY from ajayd@divensi.com forwarded another email to A.P. with the Subject heading: "Urgent Business Systems

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Engineer/Analyst in LA CA" and the message, "Please let me your view. Thanks Ajay". Contained in the email was a job opening for an unnamed end client located in Los Angeles.

k. In response to DOHRAY's email described in Paragraph 33(j), on October 2, 2013, A.P. sent an email to DOHRAY at ajayd@divensi.com with the message, "Hi Ajay, The following position is based out of LA. LA is at least 7 hrs from here. Pls fwd only relevant jobs that are based in the Bay Area."

l. On October 2, 2013, DOHRAY from ajayd@divensi.com sent an email to A.P. with the message, Yeah I remember. Now onwards I will take care of your marketing. Please follow up with me directly. Thanks Ajay"

m. From October 15, 2015 to November 15, 2013, DOHRAY from ajayd@divensi.com forwarded to A.P.'s email address a total of 11 emails for 11 different additional job openings for end clients located throughout California and Washington.

n. From the 11 additional job openings that were sent to A.P. by DOHRAY as mentioned above in Paragraph 33(m), I located an email from Collabera Senior IT Recruiter Aakash Shah to SAMAL at pksamal@azimetry.com with the Subject heading: "Work From Home Position – C++ Developer with WebGL, JavaScript experience, client location: Redmond, WA (Immediate Need)" and the message "Hi PK Samal- Please go through the complete job description below and send resume that match the job description."

o. On December 4, 2013, Divensi, Inc. Technical Recruiter Mayank Sharma from mayanks@divensi.com sent an email to A.P. with the Subject heading: "Re: Job Opportunity – Mountain View ,CA" and the message, "Hi Aruna, There is a opening of a C/C++ Engineer in Mountain View, CA

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

for a long term project. Please let me know if interested, I'll forward your details to the client."

31. Based on my training and experience and the investigation to date, I have probable cause to believe that SAMAL committed visa fraud by submitting fraudulent documents in support of A.P.'s visa petition, claiming that A.P. would be working on behalf of end client Revel when in actuality no such job offer ever existed. I also have probable cause to believe that SAMAL, DOHRAY and PUVVALA, through the use of email addresses pksamal@divensi.com, ajayd@divensi.com, prasadp@divensi.com and mayanks@divensi.com, sent emails in furtherance of an effort to commit visa fraud, by, *inter alia*, soliciting information (and payment) from A.P. prior to filing the fraudulent visa application, soliciting other potential end-clients for positions for A.P. at end clients other than Revel, Inc., requesting that A.P. submit documents and information in order to obtain a position at an end client other than Revel, Inc., and directing that A.P. actually work at end client other than Revel, Inc., notwithstanding the statements in the H1-B visa application.

b. Interview of Beneficiary G.U.

32. On January 15, 2016, IA Pinck and I interviewed G.U., one of the Divensi, Inc. beneficiaries who had been petitioned by SAMAL to work onsite at Divensi, Inc.'s office, located in Bellevue, WA. The H1-B petition for G.U. has a filing date of April 8, 2013 and an approval date of July 19, 2013. In the petition, SAMAL stated that G.U. would work on an in-house project on behalf of end client Revel. During the interview, G.U. told me that she has never worked at Divensi's office, located in Bellevue, WA or on a project for Revel, a company she had never heard of. G.U. also told me that before and after her H-1B visa petition was approved, she remained in California while Divensi, Inc.'s recruiters tried to find her projects at end clients other than Revel, Inc. G.U. told me that she eventually found a project at end client Tesla through vendor Fusion Forte where she worked as a Divensi, Inc. employee from October 7, 2013 to May 12, 2014. G.U. said that Divensi, Inc. made her pay approximately $4,500 to file her visa petition.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

33. After the interview with G.U., G.U. provided me with email correspondence between herself and Divensi, Inc. employees. In my review of those emails, and through additional investigation, I corroborated G.U.'s statements to me and observed the following evidence of visa fraud:

a. On March 19, 2013, G.U. sent an email from G.U.'s email address to Divensi, Inc. employee Mansi NAIR with the Subject heading: "Re: H1B Visa Sponsorship for 2013" and the message, "Hi Mansin, As I discussed with you myself and [S.K.] will be ready for the screening. PFA my resume."[3]

b. On March 19, 2013, Mansi NAIR from mansin@divensi.com sent an email to G.U. with a CC to her husband S.K. with the message, "Attached the Security Deposit agreement. Please sign and send it to me along with other documents. Please email me once you transfer the amount. I will update my Finance team. Thanks, Mansi NAIR Sr Technical Recruiter" Included at the bottom of the email was the account information for Azimetry, Inc.'s bank account at JP Morgan Chase.

c. On March 20, 2013, G.U. sent an email to Nair with the Subject heading: "Money Transfer from [G.U.]"[4] and the message "Hi, $4,750.00 is being transferred electronically to your account at Chase Bank. Contact me directly if you have any questions. I've chosen to have this message sent from my bank to confirm that the transfer is scheduled."

d. On March 21, 2013, NAIR from mansin@divensi.com sent an email to G.U. with the Subject heading: "FW: Money Transfer from [G.U.]"[5] and

---

[3] G.U.'s email referred to S.K. by his/her first name. In order to protect S.K.'s privacy, when quoting the contents of G.U.'s email, I have replaced S.K.'s full first name with "S.K."

[4] The subject heading of this email provided G.U.'s full first and last name. In order to protect G.U.'s privacy, when quoting the subject heading of this email, I have replaced the full name that actually appeared in the subject heading with "G.U."

[5] The subject heading of this email provided G.U.'s full first and last name. In order to protect G.U.'s privacy, when quoting the subject heading of this email, I have replaced the full name that actually appeared in the subject heading with "G.U."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the message "We have received $4,750. Thanks, Mansi Nair Sr. Technical Recruiter"

e. On January 19, 2016, G.U. sent me an email with the Subject heading: "Bank Statement Information" and a screenshot of her Bank of America statement, account number ending in 0967 showing two transfers to Azimetry, Inc. of $4,750 on March 20, 2013 and March 22, 2013 for a total of $9,000.00. When I asked G.U. why she made two payments of $4,750.00 to Azimetry, Inc., she told me the second payment was for her husband, S.K.'s petition, who will be described in greater detail below in Paragraph 38.

f. On June 24, 2013, PUVVALA from prasadp@divensi.com sent an email to G.U. with the Subject heading: "approval copy received today got for 3 years" and the message "approval copy received today got for 3 years until 09/06/2016 Thanks and Regards, Prasad V. Puvvala COO"

g. On September 26, 2013, NAIR from mansin@divensi.com sent an email to G.U. with the Subject heading: "Offer Letter and other Onboarding documents- Tesla" and the message, "Attached the offer letter and other documents. Please review the same and send us back the scanned copies. Please contact Larry Weese – larryw@divensi.com for any queries. Thanks, Mansi Nair"

h. On April 14, 2014, PUVVALA from prasadp@divensi.com sent an email to G.U. with the Subject heading: "FW: Amended LCA Compliance for [G.U.]"[6] and the message, "can u sign this also and send me back" Attached to the email is an amended LCA listing G.U.'s new end-client location as 45500 Fremont Blvd. Fremont, CA 94538. Based on a search of open source records and surveillance at the above listed address, I know

[6] The subject heading of this email provided G.U.'s full first and last name. In order to protect G.U.'s privacy, when quoting the subject heading of this email, I have replaced the full name that actually appeared in the subject heading with "G.U."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that 45500 Fremont Blvd. Fremont, CA 94538 is one of the addresses for Tesla Motors.

i. On October 2, 2013, Divensi Accounting Manager Larry Weese from larryw@divensi.com sent an email to G.U. with the Subject heading: "Welcome to Divensi" with the message "Congratulations on joining Divensi Inc. This email has a copy of our handbook attached along with some answer to frequently asked questions." Further down in the email's body, Weese writes: "How do I report my time? Please send in weekly screenshots of your approved timecard from the client's time tracking software to timecard@divensi.com . If the client does not have a time tracking solution in place, please use the attached weekly timesheet and send to your reporting manager for approval with a CC to timecard@divensi.com" Attached to the email was an Excel Spreadsheet requiring the employee to fill in the hours worked in addition to the name of the end client and project.

j. On November 15, 2013, NAIR from mansin@divensi.com sent an email to undisclosed recipients with a CC to himself at mansi.nair1@gmail.com and the message, "Going forward, please contact **PK Samal (pksamal@divensi.com)** for all your queries and concerns. He will be the single point of contact from Divensi for all your communications."

34. Based on my training and experience and the investigation to date, I have probable cause to believe that SAMAL committed visa fraud by submitting fraudulent documents in support of G.U.'s visa petition, claiming that G.U. would be working on behalf of end client Revel when in actuality no such job offer ever existed. I also have probable cause to believe that SAMAL, PUVVALA, NAIR, and WEESE, through the use of email addresses prasadp@divensi.com, mansin@divensi.com, and larryw@divensi.com, sent emails in furtherance of that visa fraud by, *inter alia*,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

requesting information (and payment) from G.U. prior to filing the fraudulent visa application, soliciting other potential end clients for positions for G.U. at end clients other than Revel, Inc., requesting that G.U. submit documents and information in order to obtain a position at an end client other than Revel, Inc., and directing that G.U. actually work at an end client other than Revel, Inc., notwithstanding the statements in the visa application.

35. I also have probable cause to believe that the email address timecard@divensi.com will contain further evidence of the "bench and switch" visa fraud scheme. As described above in Paragraph 33(i), WEESE is Divensi, Inc.'s Accounting Manager and handles all timesheets for Divensi, Inc. employees once they are placed at actual end clients. Therefore, I have probable cause to believe that the names of the companies that Divensi, Inc.'s employees are actually working at will be contained within their correspondence to email address timecard@divensi.com.

c. Interview of Beneficiary S.K.

36. On January 11, 2016, IA Pinck and I interviewed S.K., one of the Divensi, Inc. beneficiaries who had been petitioned by SAMAL to work onsite at Divensi, Inc.'s office, located in Bellevue, WA. The H1-B petition for S.K. has a filing date of April 8, 2013 and an approval date of July 3, 2013. In the petition, SAMAL alleged that S.K. would work on an in-house project on behalf of end client Revel. During the interview, S.K. told me that he has never worked at Divensi's office, located in Bellevue, WA or on a project for Revel. Once his visa was approved, he entered the U.S. from India and remained in California while Divensi, Inc.'s recruiters tried to find him a project at an end client other than Revel, Inc. S.K. told me that PUVVALA eventually found him a project at end client Tesla through vendor Fusion Forte where he worked as a Divensi, Inc. employee from November 2013 to February 15, 2015. Following the conclusion of his project at Tesla, PUVVALA found him a new end client at the Federal Reserve Bank in San Francisco where he worked as a Divensi, Inc. employee from February 16, 2015 to May 4, 2015. S.K. also told me that Divensi, Inc. made him pay a "Security Deposit" to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

file his visa petition. As already described in Paragraph 33(e), S.K.'s wife G.U. paid Divensi, Inc. a total of $9,000 for the company to file visa petitions for her and S.K.

37. After the interview with S.K., S.K. provided me with email correspondence between himself and Divensi, Inc. employees. In my review of those emails, and through additional investigation, I corroborated S.K.'s statements to me and observed the following evidence of visa fraud:

a. On November 29, 2013, Divensi, Inc. Chief Financial Officer Rory O'FLAHERTY from roryo@divensi.com sent an email to SAMAL at pksamal@divensi.com with a CC to Larry Weese at larryw@divensi.com and PUVVALA at prasadp@divensi.com with the Subject heading: "Payroll" and the message, "To all employees, Due to the Thanksgiving Holiday, our monthly wires from clients did not hit our account as expected, this will create a shorty delay in payroll processing." Based on the email's message addressing "all employees" and the fact that S.K. received this email, I believe that many of the recipients of the email, including S.K., were blind carbon copied.

b. On April 14, 2014, PUVVALA from prasadp@divensi.com sent an email to S.K. with the message "sign this amended also and send me back.."

c. On April 15, 2014, S.K. sent an email from S.K.'s email address to PUVVALA at prasadp@divensi.com with the Subject heading: "Re: FW: Amended LCA Compliance for [S.K.]"[7] and the message, "HI Prasad, PFA the attachments." Attached to the email was a letter from Divensi, Inc. attesting that S.K. was provided a copy of the LCA number I-200-13350-062035 certified by the Department of Labor, which was filed in support of his change in work site location. On January 28, 2016, I contacted Ramon

[7] The subject heading of this email provided S.K.'s full first and last name. In order to protect S.K.'s privacy, when quoting the subject heading of this email, I have replaced the full name that actually appeared in the subject heading with "S.K."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Huaracha of U.S. DOL's Wage and Hour Division and on February 1, 2016, obtained a copy of LCA number I-200-13350-062035. In my review of the amended LCA, I learned that Divensi, Inc. filed it for S.K. to work at a new end client located as 45500 Fremont Blvd. Fremont, CA 94538. As already described above in Paragraph 35(h), I know that 45500 Fremont Blvd. Fremont, CA 94538 is one of the addresses for Tesla Motors.

d. On February 23, 2015, Divensi, Inc. HR Manager Komal SINGH from komals@divensi.com sent an email to S.K. with a CC to Weese at larryw@divensi.com with the Subject heading: "Revised Compensation Letter" and the message, "The Company is pleased to inform you that your base salary has been revised w.e.f. February 2nd, 2015. The revised offer letter is annexed as part of this letter." "Thanks, Komal Singh HR Manager Divensi Inc" Attached to the email was a PDF labeled "OfferLetterRevised – [S.K.].pdf."[8] In my review of the PDF, I learned that Divensi, Inc. is paying S.K. an annual salary of $100,584.00.

e. From March 10, 2015 to May 8, 2015, S.K. sent a total of eight emails (from the email address that he/she used to send and receive the emails described in paragraphs 37(a) through (d) above) to timecard@divensi.com. Attached to each of the eight emails was a Tesla timesheet accounting for S.K.'s work at end client Tesla during the period of March 1, 2015 to May 2, 2015.

38. Based on my training and experience and the investigation to date, I have probable cause to believe that SAMAL committed visa fraud by submitting fraudulent documents in support of S.K.'s visa petition, claiming that S.K. would be working on behalf of end client Revel when in actuality no such job offer ever existed. Once the visa was approved, as described above in Paragraphs 36-37, I have probable cause to believe

[8] The file name of the attachment to this email set forth S.K.'s full first and last names. In order to protect S.K.'s privacy, when quoting the file name of the attachment to this email, I have replaced the full name that actually appeared in the file name of the attachment with "S.K."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that SAMAL, PUVVALA, O'FLAHERTY, WEESE, and SINGH, through the use of email addresses roryo@divensi.com; larryw@divensi.com; prasadp@divensi.com; komals@divensi.com; and timecard@divensi.com, sent emails in furtherance of the visa fraud by finding a position for S.K. at an end client other than Revel, Inc., requesting that S.K. complete paperwork in order to work at that end client, and asking S.K. to send completed timesheets for work performed at an end client other than Revel, Inc.

C. Investigation into Petitions Submitted by Azimetry, Inc.

39. Between on or about September 2015 and on or about February 2016, I performed an investigation into the H-1B petitions submitted by Azimetry, Inc. on behalf of foreign-worker beneficiaries who purportedly were going to work at end client GeoDigital, Inc. My investigation proceeded in two steps. First, I examined the contents and statements in actual H-1B petitions filed by Azimetry, Inc. As part of this first step, I approached GeoDigital, Inc. regarding representations about GeoDigital, Inc. that SAMAL and O'FLAHERTY made in the Azimetry, Inc. petitions, in order to determine whether those representations were accurate and whether GeoDigital, Inc. had been approached in connection with those representations. Second, I interviewed one of the sixty-five foreign-worker beneficiaries who Azimetry, Inc. identified in its petitions and interviewed him/her about his/her experience with Azimetry, Inc. and its executives, including SAMAL.

1. Review of Petitions Submitted by Azimetry, Inc.

40. On or about February 19, 2016, IA Pinck and I conducted a "Corporations Search" on the Washington State Secretary of State's website and learned that Azimetry, Inc. was incorporated in the State of Washington on August 29, 2011 and SAMAL is the company's President. On February 19, 2016, I again searched the Washington State Secretary of State's website for business records and learned that SAMAL and O'FLAHERTY are both listed as Azimetry's "Governing People" with the listed location and mailing addresses as 14320 NE 21st St. Suite 11, Bellevue, WA 98007.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

41. From on or about January 2013 to April 2015, SAMAL and O'FLAHERTY, under penalty of perjury, and through their company Azimetry, Inc., signed and submitted 66 separate I-129s and supporting documentation on behalf of 65 different foreign-worker beneficiaries to work on an alleged project for GeoDigital, Inc. The supporting documentation in the H-1B work visa petitions that accompanied the I-129s included GeoDigital, Inc. SOWs, LCAs and end-client letters attesting that the foreign workers were needed to work onsite at Azimetry's office located at 14320 NE 21st St., Suite 14 Bellevue, WA 98007 on a project on behalf of GeoDigital, Inc. The GeoDigital, Inc. end-client letters were on GeoDigital letterhead and contained Rob Murphy, GeoDigital's Director, Production Operations' alleged signature with a listed address of 775 Topaz Avenue, Unit 104, Victoria, BC V8T 4Z7.

42. On February 18, 2016, I interviewed Rob Murphy, GeoDigital's Director of Engineering Services and the alleged signatory on the 66 GeoDigital end client letters described above in Paragraph 41. After reviewing the 66 GeoDigital end client letters found in the H-1B visa petitions submitted to DHS by Azimetry, Murphy told me that he did not sign or authorize any of the letters. Murphy also told me that he did not recognize the names of any of the Azimetry employees referred to in the letters as being assigned to projects for GeoDigital, Inc.

2. Interview of Foreign-Worker Beneficiaries

a. Interview of Beneficiary V.P.

43. On January 22, 2016, DS Special Agent Matt Podolak and I interviewed V.P, one of the Azimetry, Inc. foreign-worker beneficiaries who had been petitioned by SAMAL to work onsite at Azimetry, Inc.'s office, located in Bellevue, WA. The H1-B petition for V.P. has a filing date of April 1, 2014 and an approval date of June 23, 2014. In the petition, SAMAL stated that V.P. would work on an in-house project on behalf of end client GeoDigital. During the interview, V.P. told me that she believed that she had been petitioned by Divensi, Inc. and not Azimetry, Inc. When I asked V.P. why she thought her employer was Divensi, Inc. and not Azimetry, Inc., she said it was because

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

most of the emails she received from her employer came from a Divensi, Inc. domain name. V.P. told me that she has never worked at Azimetry, Inc. or Divensi, Inc.'s offices, located in Bellevue, WA or on a project for GeoDigital or Revel. Once her visa was approved, V.P. remained in California while PUVVALA and SINGH tried to find her a project at an end client other than GeoDigital, Inc. V.P. also told me that the Subject Companies made her pay approximately $3,500 for her visa petition.

44. After the interview with V.P., V.P. provided me with email correspondence between herself and Subject Company employees. In my review of those emails, and through additional investigation, I corroborated V.P.'s statements to me and observed the following evidence of visa fraud:

a. On March 15, 2014, Komal SINGH from komals@divensi.com sent an email to V.P.'s brother with a CC to PK SAMAL at pksamal@divensi.com with the Subject heading: "H1B Questionnaire" and the message, "As discussed, please find enclosed the document and forward the same to the concerned person, will look forward to have all your documents said latest by Monday i.e, **03/17.** Thanks, Komal Singh HR Manager Divensi Inc"

b. On March 15, 2014, V.P.'s brother forwarded SINGH's email described in Paragraph 42(a) to V.P.'s email address and to the email address used by V.P.'s husband, A.P., with the message, "Please find visa document list"

c. On March 17, 2014, SINGH sent an email to V.P.'s brother with a CC to PUVVALA with the Subject heading: "SDA" and the message, "Can I please request you to get the enclosed security deposit agreement signed for all the candidates you have referred. Thanks, Komal Singh". Also attached to the email was a "Security Deposit Agreement" [SDA] from Divensi, Inc. requiring V.P. to pay $3,930 to process her H-1B visa petition.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. On May 2, 2014, SINGH from komals@divensi.com sent an email to V.P. with a CC to V.P.'s brother with the Subject heading: "Receipt Number" and the message, "**Congratulations!** We received the receipt number today from USCIS confirming that your application has been picked up in lottery for 2014 H1B petition filing."

e. On September 23, 2014, SINGH from komals@divensi.com sent an email to V.P. with the Subject heading: "FW: Job for [V.P.] – Mobile Tester – Experience with S"[9] and the message, "Just apply for this position online if you are comfortable with the JD. Thanks, Komal Singh," Included at the bottom of the email is a job description for a Quality Assurance Mobile Tester for an unnamed end client located in Seattle, WA.

f. On September 29, 2014, Divensi, Inc. Technical Recruiter Bharti GUPTA from bhartig@divensi.com sent an email to undisclosed recipients to include V.P. with the Subject heading: "SAP Tester Role" and the message, "Let me know if interested?" Included in the email is a series of emails between GUPTA and Systegration, Inc. Tech Recruiter Sofia Ortega discussing an **"SAP Automation Tester ID 28703"** project at an unnamed end client located in Redmond, WA with a start and end date of September 22, 2014 and November 14, 2014, respectively.

g. From October 17, 2014 Divensi, Inc. Technical Recruiter Hubbel ONGKING from hubbelo@divensi.com sent an email to undisclosed recipients to include V.P. with the Subject heading: "Profile" and the message, "Hello everyone, I'm not certain if I mention it before but Komal [SINGH] is transitioning back to focus on HR work. I have been assigned to continue marketing your profile along with Bharti [GUPTA]."

---

[9] The subject heading of this email set forth the first initial of V.P.'s first name and V.P.'s full last name. In order to protect V.P.'s privacy, when quoting the subject heading of this email, I have replaced the full name that actually appeared in the subject heading with "V.P."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. On October 28, 29 and 30 of 2014, ONGKING from hubbelo@divensi.com sent three emails to undisclosed recipients to include V.P. for various end client companies.

i. On January 25, 2016, V.P. sent me an email with the Subject heading: "Re: Information" and the message, "Hi Sir, Security deposit paid was 3500 $, it was check (attached) paid by brother. I have not got any email communication for refund of security deposit…" Attached to the email was a photo of a check from V.P.'s brother to Divensi, Inc. in the amount of $3,500, dated March 19, 2014. On the memo line of the check are the words "H1B – 2015[V.P.]."[10]

45. Based on my training and experience and the investigation to date, I have probable cause to believe that SAMAL committed visa fraud by submitting fraudulent documents in support of V.P.'s visa petition, claiming that V.P. would be working on behalf of end client GeoDigital when in actuality no such job offer ever existed. I also have probable cause to believe that SAMAL, PUVVALA, SINGH, GUPTA and ONGKING, through the use of email addresses komals@divensi.com; pksamal@divensi.com; bhartig@divensi.com and hubbelo@divensi.com, sent emails in furtherance of the visa fraud by, *inter alia*, soliciting information and payments from V.P. prior to filing the visa application, requesting information about positions for V.P at end clients other than GeoDigital, Inc., and asking V.P. to submit information in order to obtain a position at end clients other than GeoDigital, Inc..

VII. EVIDENCE LIKELY TO BE FOUND IN THE INFORMATION ASSOCIATED WITH THE SUBJECT EMAIL ACCOUNTS

46. Based on my investigation, I believe there are documents and records pertaining to fraudulently filed H-1B visa petitions for Subject Companies' employees contained within the Subject Email Accounts. As set out above, based on my interviews

[10] The memo line of the check used V.P.'s full first name. In order to protect V.P.'s privacy, when quoting the memo line of the check, I have replaced the full first name that actually appeared in the memo line of the check with "V.P."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of a small fraction of the foreign-worker beneficiaries for whom Divensi, Inc. and Azimetry, Inc. submitted fraudulent visa petitions, SAMAL (pksamal@divensi.com and pksamal@azimetry.com), PUVVALA (prasadp@divensi.com), O'FLAHERTY (roryo@divensi.com), NAIR (mansin@divensi.com), WEESE (larryw@divensi.com), KOMAL SINGH (komals@divensi.com), GUPTA (bhartig@divensi.com), MAYANK SINGH (mayanks@divensi.com), ONKING (hubbelo@divensi.com), and the aforementioned corporate email account to which employees were directed to send timesheets (timecard@divensi.com), all routinely sent and received emails in furtherance of the visa fraud.

47. I know from my training and experience that electronic records, such as the submission and receipt of the LCA and I-129, copies and originals of contracts, vendor letters and end client letters, are emailed from vendors and end clients to petitioning companies as attachments in PDF form, which are then saved on email accounts, computers and other electronic storage devices belonging to end clients and petitioning companies.

48. I also know from my training and experience that the people who profit and benefit from foreign worker visa frauds like this one are ordinarily the corporate officers who direct other corporate officers, corporate executives, and/or employees, often through email messages, to wittingly or unwittingly prepare or submit false statements to DHS. I know from my training and experience, and have probable cause to believe on the basis of my investigation to date, that there likely exist email messages amongst and between these listed corporate officers to the visa foreign-worker beneficiaries, and to the purported end clients Revel, Inc. and GeoDigital, Inc. which will reveal who directed and instructed the preparation and submission to DHS and DOL of the LCAs (ETA Form 9035s), I-129s and counterfeit or fraudulent supporting documentation such as third-party contracts, vendor letters, end-client and company support letters, and vendor-to-subcontractor purchase orders/contracts.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

49. Electronic information can remain on computer storage media, such as computer servers for an indefinite period of time. In my conversations with webhosts like Go Daddy and others, I have learned that it is common practice for webhosts to maintain emails indefinitely as a back-up in the event a client inadvertently deletes a message.

50. Based on my investigation and review of DHS files, and conversations with Subject Companies' employees, I know that many of Subject Companies' H-1B employees are geographically located across the nation, hundreds if not thousands of miles away. As a result, it is likely that the visa forms, internal correspondence, and correspondence with DHS and DOL were transmitted via emails with corresponding email attachments containing these documents.

51. Based on the above facts, circumstances and information, permission is requested to search the information associated with the following email accounts:

pksamal@divensi.com;
prasadp@divensi.com;
larryw@divensi.com;
roryo@divensi.com;
mansin@divensi.com;
komals@divensi.com;
timecard@divensi.com;
bhartig@divensi.com;
ajayd@divensi.com;
mayanks@divensi.com;
hubbelo@divensi.com;
pksamal@azimetry.com

VIII. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

52. Pursuant to Title 18, United States Code, Section 2703(g), this Affidavit is made in support of applications for search warrants that seek authorization to permit Go

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Daddy, and their agents and employees, to assist agents in the execution of the warrants. Once issued, the search warrants will be presented to Go Daddy with direction that they identify the Go Daddy account(s) described in Attachment A to this Affidavit, as well as other subscriber and log records associated with the account(s), as set forth in Section I of Attachment B to this affidavit.

53. The search warrants will direct Go Daddy to create exact copies of the specified accounts and records. I and/or other agents and employees of DSS and Homeland Security Investigations (HSI) will thereafter review the copies of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

54. Analyzing the data contained in the forensic images may require special technical skills, equipment, and software. It could also be very time consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common e-mail, database and spreadsheet applications do not store data as searchable text. The data is saved, instead, in proprietary non-text format. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months.

55. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant. I note, however, that based on my experience and training, in order to fully to execute the warrant, it may be necessary to review and seize all e-mail communications, chat logs and documents, that identify any users of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

subject account, and any e-mails sent or received in temporal proximity to incriminating e-mails that provide context to the incriminating communications.

IX. CONCLUSION

56. Based on the foregoing, I believe that there is probable cause that evidence, fruits, and instrumentalities of the Specified Federal Offenses is located in the Subject Email Accounts listed in Paragraph 1 and information associated with those accounts. Therefore, I respectfully request that the Court issue the proposed search warrant. Because the warrants will be served on Go Daddy, who will then compile the requested records at a time convenient to them, reasonable to cause exists to permit the execution of the requested warrants at any time in the day or night.

//
//
//
//
//
//
//
//
//
//
//
//
//
//
//
//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

X. SEALING REQUEST

57. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, Affidavit, and search warrant. Disclosure of the search warrant affidavit at this time would seriously jeopardize the ongoing investigation as the targets would not otherwise be aware of this warrant or that their activities are necessarily the subject of an ongoing criminal investigation. Disclosure at this time would provide the target with the opportunity to destroy evidence, change patterns of behavior, notify other confederates, or allow confederates to flee. Further, the investigation in this matter is continuing, and disclosing the contents of the Affidavit prior to execution will likely preclude or impede the agents and investigators working on this matter from investigating new criminal activity or leads.

Richard Lin, Special Agent
Diplomatic Security Service
U.S. Department of State
San Francisco Field Office

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 29 day of April, 2016.

BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970